

FERNANDO LOUREIRO BASTOS
(coordenador)

**IX ENCONTRO LUSO-ESPANHOL
DE PROFESSORES DE DIREITO INTERNACIONAL
E RELAÇÕES INTERNACIONAIS**

**O DIREITO INTERNACIONAL
E OS LIMITES DA LUTA
CONTRA O TERRORISMO**

**IX ENCUENTRO LUSO-ESPAÑOL
DE PROFESORES DE DERECHO INTERNACIONAL
Y RELACIONES INTERNACIONALES**

**EL DERECHO INTERNACIONAL
Y LOS LÍMITES DE LA LUCHA
CONTRA EL TERRORISMO**

2024



AA FDL
EDITORIA

Nenhuma parte desta publicação pode ser reproduzida por qualquer processo eletrônico, mecânico ou fotográfico, incluindo fotocópia, xerocópia ou gravação, sem autorização prévia do editor.

Excetuam-se as transcrições de curtas passagens para efeitos de apresentação, crítica ou discussão das ideias e opiniões contidas no livro. Esta exceção não pode, no entanto, ser interpretada como permitindo a transcrição de textos em recolhas antológicas ou similares, da qual possa resultar prejuízo para o interesse pela obra.

Os infratores são passíveis de procedimento judicial, nos termos da lei.

FERNANDO LOUREIRO BASTOS

(coordenador)

**IX ENCONTRO LUSO-ESPANHOL
DE PROFESSORES DE DIREITO INTERNACIONAL
E RELAÇÕES INTERNACIONAIS**

**O DIREITO INTERNACIONAL
E OS LIMITES DA LUTA
CONTRA O TERRORISMO**

**IX ENCUESTRO LUSO-ESPAÑOL
DE PROFESORES DE DERECHO INTERNACIONAL
Y RELACIONES INTERNACIONALES**

**EL DERECHO INTERNACIONAL
Y LOS LÍMITES DE LA LUCHA
CONTRA EL TERRORISMO**



AAEDL
EDITORA

Lisboa / 2024

Ficha Técnica**Título:**

IX Encontro Luso-Espanhol de Professores de Direito Internacional e Relações Internacionais
– O Direito Internacional e os Limites da Luta Contra o Terrorismo
AAFDL Editora – 2024

Coordenador:

Fernando Loureiro Bastos

Autores:

Ana Gascón Marcén | Carmen Parra Rodríguez | Francisco Villacampa Mejía | José Daniel
Tavares | Juan-Bautista Cartes Rodríguez | Maria do Céu Pinto Arena | Maria Francisca Saraiva |
Raquel Regueiro Dubra | Ricardo Rodrigues de Oliveira

Edição:

AAFDL Editora
Alameda da Universidade – 1649-014 Lisboa

Impressão:

AAFDL Editora

ISBN:

978-989-9252-18-9

dezembro / 2024

Nota prévia

O IX Encontro Luso-Espanhol de Professores de Direito Internacional e Relações Internacionais – *IX Encuentro Luso-Español de Profesores de Derecho Internacional y Relaciones Internacionales*, teve lugar em Lisboa, a 6 e 7 de junho de 2019, na Faculdade de Direito da Universidade de Lisboa, com o tema «O Direito Internacional e os Limites da Luta contra o Terrorismo – *El Derecho Internacional y los Límites de la Lucha contra el Terrorismo*». Foi organizado pelos Professores Doutores Maria Luísa Duarte e Fernando Loureiro Bastos, da Faculdade de Direito da Universidade de Lisboa e do *Lisbon Public Law Research Centre*/Centro de Investigação de Direito Público, e pelo Professor Doutor José Martín y Pérez de los Nanclares, da Faculdade de Direito da Universidade de Salamanca.

De acordo com a nota de divulgação do IX Encontro Luso-Espanhol de Professores de Direito Internacional e Relações Internacionais:

A 8 de setembro de 2006 a Assembleia Geral das Nações Unidas aprovou a *Estratégia Global das Nações Unidas contra o Terrorismo*, com um *Plano de Ação* baseado em quatro pilares: i) abordar as condições que propiciam a propagação do terrorismo; ii) prevenir e combater o terrorismo; iii) reforçar a capacidade dos Estados e fortalecer o papel do sistema das Nações Unidas; e iv) garantir o respeito universal pelos Direitos Humanos e pelo Estado de Direito. A 15 de junho de 2017, com o objetivo de reforçar o sistema das Nações Unidas e apoiar os seus Estados-membros na luta contra o terrorismo, foi criado o *Escritório de Luta contra o Terrorismo* (no seguimento da *Equipa Especial para a Execução da Luta contra o Terrorismo* e do *Centro das Nações Unidas contra o Terrorismo*).

Desde 1963, a Comunidade Internacional negociou e concluiu dezanove tratados internacionais para a prevenção e a repressão de atos terroristas, nos domínios da aviação civil, da proteção de pessoas com um estatuto internacional, da tomada de reféns, da proteção física de materiais nucleares, da segurança da navegação marítima, do controlo do emprego de explosivos plásticos, dos atentados terroristas com explosivos, do financiamento do terrorismo e da repressão de atos de terrorismo nuclear. Não foi possível, contudo, desde então alcançar a conclusão de um tratado geral multilateral sobre a matéria,

nomeadamente pela impossibilidade em encontrar uma definição consensual de terrorismo.

Ao nível regional europeu, a União Europeia aprovou a 30 de novembro de 2005 uma estratégia para o combate ao terrorismo identicamente baseada em quatro pilares: i) prevenir, de modo a combater a radicalização e o recrutamento de terroristas; ii) proteger os cidadãos e as infraestruturas e reduzir a vulnerabilidade a atentados; iii) perseguir, no sentido de limitar a capacidade de planeamento e a organização dos terroristas e promover a punição de atos terroristas; e iv) responder, com o objetivo de preparar, gerir e minimizar as consequências dos atentados terroristas. As medidas tomadas não conseguiram, contudo, evitar a concretização de atos de terrorismo no espaço europeu, com a consequente criação de um permanente clima de insegurança para os seus cidadãos.

Confrontados com este pano de fundo, o IX Encontro Luso-Espanhol de Professores de Direito Internacional e Relações Internacionais tem como tema de discussão os limites da luta contra o terrorismo ao nível do Direito Internacional.

A apreciação do tema do IX Encontro Luso-Espanhol será dividida em três painéis: Painel 1: A adequação do regime jurídico-internacional existente para o combate ao terrorismo; Painel 2: O financiamento do terrorismo; e Painel 3: O ciberterrorismo e a ameaça à paz e segurança internacionais.

No seguimento da nota de divulgação antes transcrita, foi aberto um *call for papers*, com as seguintes temáticas:

I – A adequação do regime jurídico-internacional existente para o combate ao terrorismo. No âmbito desta matéria podiam ser objeto de discussão nomeadamente os seguintes temas: i) As definições de terrorismo em Direito Internacional; ii) Terrorismo e o Direito da Responsabilidade Internacional; iii) Terrorismo internacional e navegação aérea; iv) Terrorismo internacional e navegação marítima; v) Terrorismo nuclear, químico e biológico em Direito Internacional; vi) Terrorismo e o Direito Internacional do Uso da Força; vii) Terrorismo e o Direito Internacional Humanitário; viii) Direito Internacional dos Direitos Humanos e Terrorismo; ix) Combate ao Terrorismo e o Direito a um julgamento justo; x) Terrorismo e o Direito Internacional dos Refugiados e das Migrações; e xi) Sistema das Nações Unidas e Combate ao Terrorismo.

II – O financiamento do terrorismo. No âmbito desta matéria podiam ser objeto de discussão nomeadamente os seguintes temas: i) Lavagem de

dinheiro e financiamento do terrorismo; ii) Balanço de vinte anos da conclusão da Convenção Internacional para a Eliminação do Financiamento do Terrorismo; iii) A estrutura institucional internacional de combate ao financiamento do terrorismo; iv) Apoio financeiro a organizações terroristas e *crowd-funding* para o financiamento de organizações terroristas; v) O financiamento do recrutamento para atos terroristas; vi) A utilização de organizações não governamentais e de outras entidades não-lucrativas para o financiamento de organizações terroristas; vii) As cripto-moedas e o financiamento do terrorismo; viii) As medidas de combate ao financiamento de atividades terroristas (congelamento e a apreensão de valores e de bens móveis e imóveis) e a salvaguarda dos direitos humanos; e ix) Financiamento do terrorismo e mercados de arte.

III – O ciberterrorismo e a ameaça à paz e segurança internacionais. No âmbito desta matéria podiam ser objeto de discussão nomeadamente os seguintes temas: i) A definição de ciberterrorismo em Direito Internacional; ii) Ciberterrorismo e cibercrime; iii) O enquadramento jurídico-internacional do ciberterrorismo; iv) A importância do ciberterrorismo no sistema contemporâneo de relações internacionais; v) O ciberterrorismo e os atores não-estaduais; vi) Ciberterrorismo e o Direito da Responsabilidade Internacional; vii) Ciberterrorismo e ciberguerra; e viii) Ciberterrorismo e a União Internacional de Telecomunicações.

O IX Encontro Luso-Espanhol de Professores de Direito Internacional e Relações Internacionais contou com a presença de professores de nove universidades espanholas (Abat Oliba CEU, Alicante, Complutense de Madrid, Huelva, Pablo de Olavide, Publica de Navarra, Salamanca, Valencia e Zaragoza), de seis universidades portuguesas (Católica do Porto, Coimbra, Lisboa, Lusíada do Porto, Minho, e Nova de Lisboa), e de um doutor pelo Instituto Universitário Europeu.

A sessão de abertura contou com as intervenções da Professora Doutora Paula Vaz Freire, subdiretora da Faculdade de Direito da Universidade de Lisboa, do Professor Doutor José Martín y Pérez de los Nanclares, da Faculdade de Direito da Universidade de Salamanca, do Professor Doutor Carlos Blanco de Moraes, Presidente do Grupo de Ciências Jurídico-Políticas da Faculdade de Direito da Universidade de Lisboa, da Professora Doutora Maria Luísa Duarte, Presidente do Instituto de Ciências Jurídico-Políticas da Faculdade de Direito da Universidade de Lisboa, e do Professor Doutor Fernando Loureiro Bastos, da Faculdade de Direito da Universidade de Lisboa.

A conferência inaugural do IX Encontro Luso-Espanhol de Professores de Direito Internacional e Relações Internacionais esteve a cargo do Professor Doutor José Martín y Pérez de los Nanclares, que fez uma intervenção com o título *Terrorismo y Unión Europea: la cuestión de los límites jurídicos en la lucha contra el terrorismo*. O Tema I, com três painéis e doze comunicações, foi apresentado pela Professora Doutora Maria do Céu Pinto Arena, com uma comunicação sobre *A governança global do terrorismo: o papel do Conselho de Segurança da ONU*. O tema II, com três comunicações, foi apresentado pela Professora Carmen Parra Rodríguez, com uma intervenção sobre *La financiación del terrorismo: principales actores, estrategias y fuentes*. O tema III, identicamente com três comunicações, foi apresentado pela Professora Doutora Sofia de Vasconcelos Casimiro, com uma apresentação sobre *O Direito Internacional e as operações em rede: os desafios do ciberterrorismo*, e pelo Professor Doutor Pedro Miguel Fernandes Freitas, com uma intervenção sobre *Cibercrime: efabulação ou realidade*. No final das sessões de trabalho, e antes da apresentação do tema do X Encontro Luso-Espanhol de Professores de Direito Internacional e Relações Internacionais, a ter lugar na Universidade de Salamanca, foi lançado o livro com as comunicações do VII Encontro Luso-Espanhol de Direito Internacional e Relações Internacionais que teve lugar em Oeiras, a 2 e 3 de junho de 2017, com a organização da Faculdade de Direito da Universidade Nova de Lisboa e da Faculdade de Direito da Universidade da Extremadura (Francisco Pereira Coutinho, Tiago de Melo Cartaxo e Juan Manuel Rodríguez Barrigón (coordenação), *Os sujeitos não estaduais no Direito Internacional*, Petrony, 2019).

O presente livro procede à publicação de oito textos elaborados no seguimento das apresentações feitas no âmbito do IX Encontro Luso-Espanhol de Professores de Direito Internacional e Relações Internacionais: i) Professora Doutora Ana Gascón Marcén, «Provedores de servicios de Internet, lucha contra el terrorismo y protección de los Derechos Humanos en la Unión Europea»; ii) Professores Doutores Carmen Parra Rodríguez e Francisco Villacampa Mejía, «La financiación del terrorismo: estructura, medios legales e ilegales y mecanismos de control»; iii) Professor Doutor José Daniel Tavares, «A indissociável relação entre o terrorismo, o branqueamento e o crime organizado»; iv) Professor Doutor Juan-Bautista Cartes Rodríguez, «Derecho Internacional Humanitario, Derecho Internacional de los Derechos Humanos y lucha contra el terrorismo: estudio de las normas convencionales de

aplicación»; v) Professora Doutora Maria do Céu Pinto Arena, «A governança global do terrorismo: o papel do Conselho de Segurança das Nações Unidas»; vi) Professora Doutora Maria Francisca Saraiva, «O Papel da Primeira Comissão da Assembleia Geral das Nações Unidas no Desenvolvimento de um Ciberespaço Estável e Seguro. Perspetivas Político-Militares sobre a Resolução “Desenvolvimentos no Campo da Informação e Telecomunicações no Contexto da Segurança Internacional”»; vii) Professora Doutora Raquel Regueiro Dubra, «La debida diligencia y el derecho de legítima defensa frente al terrorismo: especial referencia al caso de la Franja de Gaza»; e viii) Professor Doutor Ricardo Rodrigues de Oliveira, «Um olhar sobre o eco-terrorismo. Breves contributos para o Direito Internacional».

A dilação entre a realização da conferência, em junho de 2019, e a publicação dos textos que foram enviados até ao início de 2024, deveu-se à suspensão por um período considerável dos contatos académicos presenciais em resultado da Epidemia da Covid-19 e pela intenção de não interferir com a realização do X Encontro Luso-Espanhol de Professores de Direito Internacional e Relações Internacionais, que teve lugar em Salamanca, a 4 e 5 de novembro de 2022, e do XI Encontro Luso-Espanhol de Professores de Direito Internacional e Relações Internacionais, que teve lugar em Braga, a 7 e 8 de julho de 2023. Não tendo a relevância da temática do combate ao terrorismo se atenuado durante este período, antes pelo contrário, a publicação da presente obra representa um contributo dos Encontros Luso-Espanhóis de Professores de Direito Internacional e Relações Internacionais para o conhecimento e a compreensão de uma matéria de características multiformes que parece ir continuar a acompanhar-nos no futuro, o que também justifica, em termos muito reforçados, a continuação destas reuniões entre professores espanhóis e portugueses das áreas do Direito Internacional e das Relações Internacionais.

Lisboa, Faculdade de Direito da Universidade de Lisboa,
dezembro de 2024

**IX ENCONTRO LUSO-ESPANHOL DE PROFESSORES
DE DIREITO INTERNACIONAL
E RELAÇÕES INTERNACIONAIS**

**IX ENCUESTRO LUSO-ESPAÑOL DE PROFESORES
DE DERECHO INTERNACIONAL
Y RELACIONES INTERNACIONALES**

**Lisboa, 6 e 7 de junho de 2019 – Lisboa, 6 y 7 de junio de 2019
Faculdade de Direito da Universidade de Lisboa**

**O DIREITO INTERNACIONAL E OS LIMITES
DA LUTA CONTRA O TERRORISMO**

**EL DERECHO INTERNACIONAL Y LOS LÍMITES
DE LA LUCHA CONTRA EL TERRORISMO**

Programa do Encontro

6 de junho de 2019

14:00-14:30 – Registo dos participantes

**14:30 – 15:00 – Abertura do IX Encontro Luso-Espanhol de Professores
de Direito Internacional e Relações Internacionais**

– Paula Vaz Freire – Subdiretora da Faculdade de Direito da Universidade
de Lisboa

– José Martín y Pérez de los Nanclares – Faculdade de Direito da
Universidade de Salamanca

– Carlos Blanco de Moraes – Presidente do Grupo de Ciências
Jurídico-Políticas da Faculdade de Direito da Universidade de Lisboa

– Maria Luísa Duarte – Presidente do Instituto de Ciências Jurídico-
-Políticas da Faculdade de Direito da Universidade de Lisboa

– Fernando Loureiro Bastos – Faculdade de Direito da Universidade
de Lisboa

15:00 – 15:45 – Conferência Inaugural

José Martín y Pérez de los Nanclares – Terrorismo y Unión Europea: la cuestión de los límites jurídicos en la lucha contra el terrorismo

15:45 – 17:15 – Tema I – Painel I – A adequação do regime jurídico-internacional existente para o combate ao terrorismo

Modera: Maria Luísa Duarte

Apresentação geral do tema:

Maria do Céu Pinto Arena, *A governança global do terrorismo: o papel do Conselho de Segurança da ONU*, Universidade do Minho (20 minutos)

Comunicações (15 minutos cada)

Raquel Regueiro Dubra – La debida diligencia como requisito para la atribución en el marco del artículo 51 de la Carta de las Naciones Unidas: *Aliquid novo sub solo?* – Universidade Complutense de Madrid

Alicia Chicarro Lázaro – Atribución de la responsabilidad internacional por actividades terroristas de alcance transnacional – Universidade Pública de Navarra

Emellin de Oliveira – Migração e terrorismo: a tecnologia como instrumento de combate à ameaça terrorista? – Universidade Nova de Lisboa

Debate

17:15-17:45 – Pausa

17:45-18:45 Tema I – Painel II – A adequação do regime jurídico-internacional existente para o combate ao terrorismo

Modera: Rui Guerra da Fonseca

Comunicações (15 minutos cada)

Maria Francisca Saraiva – O papel da Primeira Comissão da Assembleia Geral das Nações Unidas no enquadramento político-militar do ciberespaço. Perspetivas sobre a resolução “Desenvolvimentos no campo da informação e telecomunicações no contexto da segurança internacional” – Universidade de Lisboa

Pilar Pozo Serrano – El uso de drones armados en la lucha contra el terrorismo: problemas de Derecho Internacional – Universidade de Valência (Professora Titular)

Programa do Encontro

Vasco Becker-Weinberg – O terrorismo e o uso da força no mar –
Universidade Nova de Lisboa

Debate

20:00 Jantar (participação facultativa mediante inscrição prévia)

7 de junho de 2019

10:00 – 13:00 – Tema I – Painel III – A adequação do regime jurídico-internacional existente para o combate ao terrorismo

Modera: Fernando Loureiro Bastos

Comunicações (15 minutos cada)

David López Calderon – La lucha contra el Estado Islámico a la luz del Derecho internacional: há sido eficaz la labor de Naciones Unidas? – Universidade de Salamanca

Tiago de Melo Cartaxo – Horizontes do terrorismo ambiental: o caso do conflito entre Paquistão e Índia – Universidade Nova de Lisboa

Ricardo Rodrigues de Oliveira – Um olhar sobre o eco-terrorismo. Uma realidade pouco estudada e com insuficiente proteção jurídico-internacional – Instituto Universitário Europeu

Debate

11:15-11:30 – Pausa

Comunicações (15 minutos cada)

Ana Soares Pinto – Terrorismo e Direito Internacional Humanitário – Universidade de Lisboa

Juan Bautista Cartes Rodríguez – La aplicación del Derecho Internacional de los Derechos Humanos a grupos armados terroristas: una vía a tener en cuenta para colmar algunos de los vacíos jurídicos existentes? – Universidade Complutense de Madrid

Sónia Roque – O Conselho de Direitos Humanos e a proteção de civis na luta contra o terrorismo – Universidade de Coimbra

Debate

13:00 – 14:30 – Almoço

14:30 – 16:00 – Tema II – O financiamento do terrorismo

Modera: Wladimir Brito

Apresentação geral do tema:

Carmen Parra Rodriguez, La financiación del terrorismo: principales actores, estrategias y fuentes – Universidade Abat Oliba CEU (20 minutos)

Comunicações (15 minutos cada)

Jorge Urbaneja Cillían – Nuevos instrumentos financeiros y prevención de la financiación del terrorismo – Universidade de Alicante

Carmen Parra Rodriguez e Francisco Villacampa Megia – La Financiación del terrorismo a través del tráfico ilícito de bienes culturales – Universidade Abat Oliba CEU

José Daniel Tavares – A indissociável relação entre o terrorismo, o branqueamento e o crime organizado – Universidade Lusíada do Porto

Debate

16:00-16:30 – Pausa

16:45-18:30 – Tema III – O ciberterrorismo e a ameaça à paz e segurança internacionais

Modera: Manuel Almeida Ribeiro

Apresentação geral do tema:

Sofia de Vasconcelos Casimiro, O Direito Internacional e as operações em rede: os desafios do ciberterrorismo – Universidade de Lisboa (20 minutos)

Pedro Miguel Fernandes Freitas, Cibercrime: efabulação ou realidade, Universidade Católica – Porto (20 minutos)

Comunicações (15 minutos cada)

Ana Cristina Gallego Hernández – El ciberterrorismo y la salud – Universidade Pablo de Olavide/Universidade de Huelva

Ana Gascón Marcén – Intermediarios de internet, lucha contra el terrorismo y derechos humanos – Universidade de Zaragoza

Rui Tavares Lanceiro e Paulo Simões Ramos – *Where there is smoke, there is fire*: a atribuição de atos internacionalmente ilícitos a Estados no contexto de ciberoperações conduzidas por agentes não-estatais – Universidade de Lisboa

Debate

18:30-18:45 – Lançamento do livro com as conferências e as comunicações do VII Encontro Luso-Espanhol (Lisboa)

18:45-19:15 – Apresentação do tema do X Encontro Luso-Espanhol e encerramento do IX Encontro Luso-Espanhol

– José Martín y Pérez de los Nanclares – Faculdade de Direito da Universidade de Salamanca

– Fernando Loureiro Bastos – Faculdade de Direito da Universidade de Lisboa

– Maria Luísa Duarte – Presidente do Instituto de Ciências Jurídico-Políticas da Faculdade de Direito da Universidade de Lisboa

Índice

Ana Gascón Marcén	21
Provedores de servicios de Internet, lucha contra el terrorismo y protección de los Derechos Humanos en la Unión Europea <i>Internet service providers, the fight against terrorism and the protection of human rights in the European Union</i>	
Carmen Parra Rodríguez Francisco Villacampa Mejía	65
La financiación del terrorismo: estructura, medios legales e ilegales y mecanismos de control <i>Terrorist financing: structure, legal and illegal means and control mechanisms</i>	
José Daniel Tavares	103
A indissociável relação entre o terrorismo, o branqueamento e o crime organizado <i>The indissociable relationship between terrorism, money laundering and organized crime</i>	
Juan-Bautista Cartes Rodríguez	131
Derecho Internacional Humanitario, Derecho Internacional de los Derechos Humanos y lucha contra el terrorismo: estudio de las normas convencionales de aplicación <i>International Humanitarian Law, International Human Rights Law and the fight against terrorism: a study of the conventional norms of application</i>	
Maria do Céu Pinto Arena	169
A governança global do terrorismo: o papel do Conselho de Segurança das Nações Unidas <i>The global governance of terrorism: the role of the United Nations Security Council</i>	

Maria Francisca Saraiva	181
O Papel da Primeira Comissão da Assembleia Geral das Nações Unidas no Desenvolvimento de um Ciberespaço Estável e Seguro. Perspetivas Político-Militares sobre a Resolução “Desenvolvimentos no Campo da Informação e Telecomunicações no Contexto da Segurança Internacional”	
<i>The Role of the United Nations General Assembly First Committee in Developing a Stable and Secure Cyberspace. Political and Military Perspectives on the Resolution “Developments in the Field of Information and Telecommunications in the Context of International Security”</i>	
Raquel Regueiro Dubra	203
La debida diligencia y el derecho de legítima defensa frente al terrorismo: especial referencia al caso de la Franja de Gaza	
<i>Due diligence and the right of self-defense against terrorism: special reference to the case of the Gaza Strip</i>	
Ricardo Rodrigues de Oliveira	235
Um olhar sobre o eco-terrorismo. Breves contributos para o Direito Internacional	
<i>Shedding light on eco-terrorism. Brief contributions to International Law</i>	

Autores

ANA GASCÓN MARCÉN

Profesora Contratada Doctora de la Facultad de Derecho de la Universidad de Zaragoza y miembro del equipo de investigación del proyecto «Hacia una transición digital centrada en la persona en la Unión Europea»; esta publicación es parte del proyecto TED2021-129307A-I00, financiado por MCIN/AEI/10.13039/501100011033 y por la Unión Europea “NextGenerationEU”/PRTR.

CARMEN PARRA RODRÍGUEZ

Profesora Titular de Derecho internacional privado de la Universidad Abat Oliba CEU. Directora de la Cátedra Unesco Paz, Solidaridad y Diálogo Intercultural – cparra@uao.es

FRANCISCO VILLACAMPA MEJÍA

Profesor de Derecho internacional público de la Universidad Abat Oliba CEU. Director de Estudios del Grado de Criminología y Vicedecano de la Facultad de Derecho y Economía – fvillacampam@uao.es

JOSÉ DANIEL TAVARES

Professor Auxiliar do Centro Universitário Lusíada – Norte / Porto – danieltavares32@sapo.pt

JUAN-BAUTISTA CARTES RODRÍGUEZ

Profesor de Derecho Internacional de la Universidad Complutense de Madrid. Premio Extraordinario de Doctorado. Premio J. Brunet a la Mejor Tesis Doctoral de España sobre Derechos Humanos

MARIA DO CÉU PINTO ARENA

Doutora em Ciência Política e Relações Internacionais pela Universidade de Durham, Reino Unido/Universidade do Minho e Professora Associada com Agregação do Departamento de Ciência Política da Universidade do Minho

MARIA FRANCISCA SARAIVA

Professora Auxiliar do Instituto Superior de Ciências Sociais e Políticas (ISCSP) da Universidade de Lisboa. Investigadora do Centro de Administração e Políticas Públicas do ISCSP, do Instituto da Defesa Nacional e do Instituto Universitário Militar – msaraiva@iscsp.ulisboa.pt

RAQUEL REGUEIRO DUBRA

Professora Contratada Doctora no Departamento de Derecho Internacional, Derecho Eclesiástico y Filosofía da Universidad Complutense de Madrid. Doutora em Direito pela Universidad Complutense de Madrid (*cum laude* por unanimidad) e Licenciada em Direito pela Universidade de Genebra, onde também obteve um Diploma em Direito Transnacional.

RICARDO RODRIGUES DE OLIVEIRA

Professor auxiliar convidado e investigador contratado da Universidade Católica Portuguesa, Faculdade de Direito, *Católica Research Centre for the Future of Law*, Portugal. Investigador colaborador do *Lisbon Public Law Research Centre* da Faculdade de Direito da Universidade de Lisboa – rroliveira@ucp.pt

Proveedores de servicios de Internet, lucha contra el terrorismo y protección de los derechos humanos en la Unión Europea

Internet service providers, the fight against terrorism and the protection of human rights in the European Union

Ana Gascón Marcén

Resumen: Los proveedores de servicios de Internet se han convertido en actores claves para luchar contra el terrorismo en el ámbito digital, no obstante, su implicación debe realizarse siempre respetando una serie de salvaguardas de derechos fundamentales. En este trabajo, se analizan dos aspectos en los que su actuación es relevante, como son, por una parte, la moderación de contenidos, prestando especial atención al Reglamento para la prevención de la difusión de contenidos terroristas en línea de la Unión Europea y, por otra parte, a la obtención y acceso a pruebas electrónicas, empezando con la recogida de las mismas respondiendo a obligaciones de conservación de datos y la jurisprudencia europea al respecto, para luego pasar a lo relativo al acceso transfronterizo a pruebas electrónicas.

Palabras clave: intermediarios de Internet; terrorismo; derechos humanos; pruebas electrónicas.

Abstract: Internet service providers have become key players in the fight against terrorism in the digital sphere, however, their involvement must always be carried out in compliance with a series of fundamental rights safeguards. This paper analyses two aspects in which their action is relevant, namely, on the one hand, content moderation, paying special attention to the Regulation for the prevention of the dissemination of terrorist content online of the European Union and, on the other hand, obtaining and accessing electronic evidence, starting with the collection of the same in response to data retention obligations and the European case-law on the subject, and then moving on to the cross-border access to electronic evidence.

Keywords: Internet intermediaries; terrorism; human rights; electronic evidence.

Sumario: 1. Introducción; 2. Reglamento para la prevención de la difusión de contenidos terroristas en línea; 3. Pruebas electrónicas; 3.1 Conservación de datos; 3.2 Acceso transfronterizo a pruebas electrónicas para investigaciones penales; 4. Conclusiones.

1. Introducción

Internet es una magnífica herramienta para ejercer la libertad de expresión y el derecho a la información, así como otros muchos derechos y libertades, pero también puede ser usada para delinquir. En particular, resulta muy útil para los terroristas porque les permite reclutar, planear y facilitar sus actividades, ser una herramienta de adiestramiento, obtener financiación y recursos (incluidas armas), glorificar sus actos, difundirlos e insuflar el miedo en la opinión pública dando un altavoz a su mensaje¹. Internet es especialmente apropiada por varias de sus características como ser un medio rápido, descentralizado, sin barreras de acceso, con un público potencial altísimo y la posibilidad de encriptar las comunicaciones².

Para limitar este uso de Internet por parte de los terroristas es necesaria la colaboración de los Estados con los proveedores de servicios de Internet, lo que a nivel global se ha canalizado a través del *Christchurch Call*.³ Son

¹ BRANISLAV TODOROVIC y DARKO TRIFUNOVIC, «Chapter 19. Prevention of (Ab-)Use of the Internet for Terrorist Plotting and Related Purposes», *Handbook of Terrorism Prevention and Preparedness*, ICCT Press, La Haya, 2020, pp. 616-643; y MAURA CONWAY ET AL. (eds.), *Terrorist use of the Internet*, OTAN, 2017.

² TECH AGAINST TERRORISM, *Trends in Terrorist and Violent Extremist Use of the Internet. Q1-Q2 2021*, 2021, disponible en <https://www.techagainstterrorism.org/wp-content/uploads/2021/07/Tech-Against-Terrorism-Q1-Q2-TVEC-Trends-2021.pdf> (última consulta: 18-09-23).

³ El 15 de marzo de 2019, se transmitió en directo un ataque terrorista contra dos mezquitas en Christchurch (Nueva Zelanda). 51 personas murieron y 50 resultaron heridas. La transmisión fue vista en directo por menos de 200 personas, pero 4.000 personas la vieron antes de que Facebook la retirara y rápidamente se hizo viral, siendo reproducida en muchas otras páginas. En total, Facebook eliminó alrededor de 1,5 millones de videos del ataque a nivel mundial en las primeras 24 horas Véase GRAHAM MACKLIN, «The Christchurch attacks: Livestream terror in the viral video age», *CTC Sentinel*, vol. 12, t. 6, 2019, pp. 18-29.

múltiples las organizaciones internacionales que fomentan la colaboración con los proveedores para luchar contra el terrorismo en Internet, como el Consejo de Europa⁴ o las Naciones Unidas⁵. No obstante, este trabajo se centrará en la actuación de la Unión Europea (UE).

Uno de sus primeros pasos fue la creación del Foro de Internet de la UE en 2005 que reúne cada año a representantes de los gobiernos, Europol y empresas de tecnología para coordinarse y combatir el contenido terrorista⁶.

Como respuesta, el 15 de mayo de 2019, la primera ministra de Nueva Zelanda, Jacinda Ardern, y el presidente francés, Emmanuel Macron, reunieron a jefes de Estado y de gobierno y líderes del sector tecnológico para adoptar el *Christchurch Call*. Se trata de un compromiso para eliminar el contenido terrorista y extremista violento en línea. Un gran número de Estados y empresas decidieron sumarse y además se creó una red consultiva compuesta por grupos de la sociedad civil, que representan una variedad de perspectivas, incluidos los derechos humanos, la lucha contra la radicalización, y el apoyo a las víctimas.

⁴ En 2017, el Consejo de Europa lanzó un marco general para trabajar con empresas de Internet y sus asociaciones representativas, que les permite participar en una variedad de actividades de la organización y sentarse junto con los gobiernos en la elaboración de políticas digitales. Actualmente, 27 actores de la industria se han sumado a este marco. Véase Council of Europe's Digital Partnership, 2022 <https://rm.coe.int/10-06-2022-digital-partnership-general-doc-updated/1680a6e634> (última consulta: 18-09-23).

⁵ Por ejemplo, la Relatora especial sobre la promoción y la protección de los derechos humanos y las libertades fundamentales en la lucha contra el terrorismo se ha dirigido directamente a Facebook para discutir su definición de terrorismo y hacerle recomendaciones para mejorar sus procesos en lo que se refiere a la transparencia, la seguridad jurídica y los remedios en caso de violación de derechos. Véase su carta al Sr. Zuckerberg de 24 de julio de 2018, OL OTH 46/2018 https://www.ohchr.org/sites/default/files/Documents/Issues/Terrorism/OL_OTH_46_2018.pdf (última consulta: 18-09-23) y también mandó observaciones al Facebook Oversight Board véase Input to the Facebook Oversight Board on Community and Community Standard on Dangerous Individuals and Organizations de 2021.

⁶ COMISIÓN EUROPEA, «EU Internet Forum: Bringing together governments, Europol and technology companies to counter terrorist content and hate speech online», Press release, Bruselas, 3-12-2015. Este Foro ha promovido la creación de una base de más de 200.000 *hashes* que sirve para evitar que los vídeos o fotografías ya etiquetados como contenido terrorista puedan volver a compartirse. Además, en 2019, adoptó un Protocolo de crisis para proporcionar una respuesta rápida para contener la propagación viral de contenido terrorista y extremista violento en línea. COMISIÓN EUROPEA, *A Europe that protects EU Crisis Protocol: responding to terrorist content online*, 2019, disponible en https://ec.europa.eu/home-affairs/sites/default/files/what-we-do/policies/european-agenda-security/20191007_agenda-security-factsheet-eu-crisis-protocol_en.pdf (última consulta: 18-09-23). Citron ha argumentado que estas medidas que fomentan la asunción por parte de los intermediarios de medidas «voluntarias» puede conllevar un «*cancelship creep*» que suponga que una amplia

En 2015, se creó la Unidad de Notificación de Contenidos de Internet de Europol que forma parte del Centro Europeo de Lucha contra el Terrorismo. Su mandato incluye notificar contenido terrorista y extremista violento a los proveedores de servicios en línea para que lo eliminen⁷ y la prestación de apoyo a los Estados miembros y terceros en el contexto de las investigaciones en Internet⁸. El Consejo Europeo declaró en 2017 que la industria debía hacer más para ayudar a combatir el terrorismo en línea⁹.

Los proveedores de servicios de Internet deben conciliar este objetivo legítimo con el de respetar los derechos humanos, conforme a los Principios Rectores sobre Empresas y Derechos Humanos, respaldados por el Consejo de Derechos Humanos en 2011. Estos Principios reconocen que los Estados son los principales sujetos obligados a respetar, proteger y cumplir los estándares de derechos humanos y las libertades fundamentales, lo que significa no sólo que no deben infringirlos, sino también que deben crear un marco legal donde las empresas tampoco puedan hacerlo. El papel de las empresas como órganos de la sociedad que realizan funciones especializadas (como es el caso de los intermediarios de Internet) les exige cumplir con todas las leyes aplicables y respetar los derechos humanos.¹⁰ La cuestión es cómo aplicar estos principios generales a los intermediarios de Internet en su lucha contra el terrorismo en línea.

gama de discursos protegidos, incluida la crítica política y el contenido de interés periodístico, pueden terminar siendo eliminados de las plataformas en línea a escala global DANIELLE KEATS CITRON, *What to Do about the Emerging Threat of Censorship Creep on the Internet*, Cato Institute, 28-11-2017, disponible en <https://www.cato.org/policy-analysis/what-do-about-emerging-threat-censorship-creep-internet> (última consulta: 18-09-23) y de la misma autora *Extremist Speech, Compelled Conformity, and Censorship Creep*, University of Maryland Francis King Carey School of Law Legal Studies Research Paper No. 2017-12.

⁷ Por ejemplo, en 2021 realizó 19573 notificaciones de contenidos terroristas. Véase EUROPOL, *EU IRU Transparency Report 2021*, 2022. Disponible en https://www.europol.europa.eu/cms/sites/default/files/documents/EU_IRU_Transparency_Report_2021.pdf (última consulta: 18-09-23).

⁸ Por ejemplo, cada año realiza un informe sobre la propaganda yihadista en línea. Véase EUROPOL, *Online Jihadist Propaganda 2021 in review*, Publications Office of the European Union, Luxemburgo, 2022.

⁹ Conclusiones del Consejo Europeo de 22 y 23 de junio de 2017. EUCO 8/17.

¹⁰ Véase ANA GASCÓN MARCÉN, «Los intermediarios de internet y la protección de los derechos humanos», *Las empresas transnacionales en el derecho internacional contemporáneo: Derechos humanos y objetivos de desarrollo sostenible*, Tirant lo Blanch, 2019, pp. 399-412.

En este trabajo nos vamos a centrar en dos aspectos en los que los intermediarios de Internet pueden verse compelidos a luchar contra el terrorismo, por una parte está la moderación de contenidos y en ese sentido se prestará especial atención al Reglamento para la prevención de la difusión de contenidos terroristas en línea de la UE (apartado 2), y en lo referente a las pruebas electrónicas (apartado 3) empezaremos analizando la recogida de pruebas con las obligaciones de conservación de datos de los intermediarios y la jurisprudencia europea al respecto (sección 3.1) para luego pasar a lo relativo al acceso transfronterizo a pruebas electrónicas (sección 3.2), para terminar con unas breves conclusiones (apartado 4).

2. Reglamento para la prevención de la difusión de contenidos terroristas en línea

La Directiva (UE) 2017/541 estableció que los Estados miembros debían adoptar las medidas necesarias para garantizar la rápida eliminación de los contenidos en línea albergados en su territorio constitutivos de provocación pública a la comisión de un delito de terrorismo. Además, debían procurar obtener la eliminación de tales contenidos cuando estuvieran albergados fuera de su territorio.

La Comisión Europea adoptó comunicaciones y recomendaciones¹¹ para fomentar que los intermediarios lucharan contra los contenidos ilícitos en línea incluidos los contenidos terroristas.¹² No obstante, se constató que los compromisos voluntarios de los intermediarios no eran suficientemente efectivos. A esto se sumó que varios Estados se plantearon adoptar sus propias normas que tenían por objetivo obligar a los intermediarios a retirar contenidos

¹¹ *Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones. Lucha contra el contenido ilícito en línea. Hacia una mayor responsabilización de las plataformas en línea*, COM(2017) 555 final y COMISIÓN EUROPEA, Recomendación (UE) 2018/334 de la Comisión de 1 de marzo de 2018 sobre medidas para combatir eficazmente los contenidos ilícitos en línea. DOUE L 63/50 6-3-2018.

¹² *Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones. Lucha contra el contenido ilícito en línea. Hacia una mayor responsabilización de las plataformas en línea*, COM(2017) 555 final y Recomendación (UE) 2018/334 de la Comisión de 1 de marzo de 2018 sobre medidas para combatir eficazmente los contenidos ilícitos en línea. DOUE L 63/50 6-3-2018.

ilícitos en unos plazos limitados, lo que podía suponer la fragmentación del mercado único digital. Además, Francia y Alemania instaron a la Comisión a que presentara una iniciativa legislativa para luchar contra los contenidos terroristas en Internet¹³.

Hasta ese momento realmente los intermediarios de Internet no eran responsables de los contenidos terroristas que terceros compartieran a través de los mismos siempre que cumplieran con los requisitos establecidos en la Directiva de Comercio Electrónico¹⁴. Las condiciones eran que el intermediario no contralara el contenido y no tuviera conocimiento efectivo de que la información era ilícita y que, en cuanto tuviera conocimiento de la ilicitud, actuara con prontitud para retirar los datos o hacer que el acceso a ellos fuera imposible. Además, la Directiva prohibía a los Estados imponer a los prestadores de servicios una obligación general de supervisar los datos que transmitieran o almacenaran, o una obligación general de realizar búsquedas activas de hechos o circunstancias que indicaran actividades ilícitas (incluidas las terroristas). No obstante, la UE ha ido matizando en los últimos años estas exenciones a través de normativa sectorial en ámbitos concretos como la protección de los derechos de autor o las comunicaciones audiovisuales.

En 2021, la UE adoptó el Reglamento sobre la lucha contra la difusión de contenidos terroristas en línea.¹⁵ Esta norma establece normas uniformes con el fin de luchar contra el uso indebido de los servicios de alojamiento de datos para la difusión entre el público de contenidos terroristas en línea, en particular: los deberes razonables y proporcionados de diligencia que deben aplicar los prestadores de servicios de alojamiento de datos (en adelante prestadores) para luchar contra la difusión entre el público de contenidos

¹³ *Carta conjunta de los ministros de interior francés y alemán a varios comisarios europeos*, 12-4-2018, disponible en https://edri.org/files/censorship_fr.pdf (última consulta: 18-09-23).

¹⁴ Directiva 2000/31/CE del Parlamento Europeo y del Consejo, de 8 de junio de 2000, relativa a determinados aspectos jurídicos de los servicios de la sociedad de la información, en particular el comercio electrónico en el mercado interior (Directiva de Comercio Electrónico), DOUE L178, 17-7-2000, pp. 1-16.

¹⁵ Reglamento (UE) 2021/784 del Parlamento Europeo y del Consejo, de 29 de abril de 2021, sobre la lucha contra la difusión de contenidos terroristas en línea, DOUE L 172, 17.5.2021, p. 79–109. Véase ANA GASCÓN MARCÉN, «El nuevo Reglamento europeo para la prevención de contenidos terroristas en línea», *Retos del Estado de Derecho en materia de inmigración y terrorismo*, Iustel, 2022, pp. 525-546.

terroristas a través de sus servicios y garantizar la retirada o el bloqueo de acceso rápidos a dichos contenidos; y las medidas que deben tomar los Estados miembros, de conformidad al Derecho de la UE y a reserva de las salvaguardias adecuadas para proteger los derechos fundamentales, en particular la libertad de expresión e información en una sociedad abierta y democrática, con el fin de detectar y permitir la retirada rápida de los contenidos terroristas por parte de los prestadores, y facilitar la cooperación entre las autoridades competentes de los Estados miembros, los prestadores y Europol.

La propuesta de la Comisión definía los contenidos terroristas como aquellos que inciten a la comisión de delitos de terrorismo o los defiendan, incluidos los que hagan apología de ellos, provocando con ello un peligro de comisión de dichos actos; los que fomenten la contribución a delitos de terrorismo; los que promuevan las actividades de un grupo terrorista, en particular fomentando la participación en un grupo terrorista o el apoyo al mismo; y los que instruyan sobre métodos o técnicas para la comisión de delitos de terrorismo.

La definición de lo que es terrorismo ha sido históricamente complicada y lo mismo ocurre con esta definición de «contenidos terroristas» que fue muy criticada por ser demasiado amplia¹⁶, pero las críticas no sólo provenían de la universidad o de ONG, sino que varios relatores de Naciones Unidas mandaron sendas cartas a la UE en 2018 y 2020 muy preocupados con la propuesta entre otras cuestiones por este punto¹⁷. En su opinión, que la

¹⁶ JOAN BARATA, *New EU Proposal on the Prevention of Terrorist Content Online*, Center for Internet and Society, 2018, pp. 4 y 5; GERMÁN MANUEL TERUEL LOZANO, «Una lectura garantista de las nuevas tendencias en la lucha europea contra la difusión de mensajes terroristas en Internet», *Revista de Derecho Constitucional Europeo*, vol. 34. Julio-Diciembre de 2020; y ALEKSANDRA KUCZERAWY, *The proposed Regulation on preventing the dissemination of terrorist content online: safeguards and risks for freedom of expression*, Center for Democracy and Technology, 2018.

¹⁷ *Joint letter of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression; the Special Rapporteur on the right to privacy and the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism*, OL OTH 71/2018, 7-12-2018, disponible en <https://spcommreports.ohchr.org/TMResultsBase/DownloadPublicCommunicationFile?gId=24234> (última consulta: 18-09-23); y *Joint letter of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression and the Special Rapporteur on the promotion and protection*

Comisión siguiera las definiciones de la Directiva (UE) 2017/541 ya presentaba ciertos problemas, pero es que la propuesta además iba mucho más allá. La propia Agencia de Derechos Fundamentales de la UE recomendó mejorar el respeto por los derechos fundamentales proporcionando una definición clara de contenido terrorista y su difusión, mejorando la previsibilidad y claridad de la definición, limitando claramente el alcance de la propuesta a los contenidos difundidos al público y excluyendo determinadas formas de expresión del ámbito de la propuesta¹⁸.

Tras las negociaciones para su adopción entre el Parlamento y el Consejo, en el texto definitivo de la norma se excluyó de la definición el material que «promueve» las actividades de grupos terroristas y se ajustó más estrechamente a los delitos pertinentes de la Directiva relativa a la lucha contra el terrorismo. Quedando como sigue: uno o más de los siguientes tipos de material que incite a la comisión de uno de los delitos a que se refiere el artículo 3.1, letras a) a i), de la Directiva (UE) 2017/541, cuando tal material preconice directa o indirectamente a través por ejemplo de la apología de actos terroristas, la comisión de delitos de terrorismo, generando con ello un riesgo de que se puedan cometer uno o varios de dichos delitos; induzca a una persona o grupo de personas a cometer o contribuir a la comisión de los delitos a que se refiere el artículo 3.1, letras a) a i), de la Directiva (UE) 2017/541; induzca a una persona o grupo de personas a participar en las actividades de un grupo terrorista en el sentido del artículo 4.b de la Directiva (UE) 2017/541; proporcione instrucción sobre la fabricación o el uso de explosivos, armas de fuego u otras armas o sustancias nocivas o peligrosas, o sobre otros métodos o técnicas específicos cuyo fin sea la comisión o la contribución a la comisión de cualquiera de los delitos de terrorismo a que se refiere el artículo 3.1, letras a) a i), de la Directiva (UE) 2017/541; o constituya una amenaza de comisión de los delitos a que se refiere el artículo 3.1, letras a) a i), de la

of human rights and fundamental freedoms while countering terrorism, OL OTH 73/2020, 3-11-2020, disponible en <https://spcommreports.ohchr.org/TMResultsBase/DownloadPublicCommunicationFile?gId=25661> (última consulta: 18-09-23).

¹⁸ *Opinion of the European Union Agency for Fundamental Rights 2/2019 on the Proposal for a Regulation on preventing the dissemination of terrorist content online and its fundamental rights implications*, 12-2-2019, disponible en https://fra.europa.eu/sites/default/files/fra_uploads/fra-2019-opinion-online-terrorism-regulation-02-2019_en.pdf (última consulta: 18-09-23).

Directiva (UE) 2017/541. No obstante, Scheinin consideró esta definición problemática porque «las decisiones algorítmicas o administrativas para ordenar la eliminación inmediata de Internet de contenido terrorista no pueden, ni en la lógica ni en la práctica, basarse en criterios que se han escrito para ser determinados a través de la acusación contradictoria basada en la evidencia del proceso de un juicio penal»¹⁹.

Respecto al ámbito de aplicación, se aclaró que el material difundido con fines educativos, periodísticos, artísticos o de investigación, o con fines de prevención o lucha contra el terrorismo, no debe considerarse contenido terrorista, y que una evaluación debe determinar la verdadera finalidad de la difusión. Esto es una garantía importante porque, por ejemplo, el uso de hashes para identificar y bloquear contenido que, en algunos contextos, puede considerarse «propaganda terrorista» puede no tener en cuenta situaciones en las que dicho contenido se comparte para documentar abusos de derechos humanos o para proporcionar cobertura periodística²⁰.

Se criticó la propuesta por ser muy amplio su ámbito de aplicación, o sea, sus destinatarios, ya que los prestadores realizan labores muy diversas. Aunque el texto definitivo de la norma especificó que se aplica solo a los que difunden información al público (a un número potencialmente ilimitado de personas), así quedaría fuera, por ejemplo, los proveedores de servicios de alojamiento en la nube. Sin embargo, según van Hoboken, el foco se sitúa en la capacidad de los proveedores para actuar como puntos de control y censores de la expresión en línea, sin tener en cuenta el papel preciso que juegan los diferentes servicios en el entorno en línea y su relación con las actividades expresivas que ayudan a facilitar.²¹

¹⁹ MARTIN SCHEININ, «The EU Regulation on Terrorist Content: An Emperor without Clothes», *Verfassungsblog*, 30-1-2019, disponible en <https://verfassungsblog.de/the-eu-regulation-on-terrorist-content-an-emperor-without-clothes/> (última consulta: 18-09-23).

²⁰ HUMAN RIGHTS WATCH, «*Video Unavailable*»: *Social Media Platforms Remove Evidence of War Crimes*, Human Rights Watch. 2020, disponible en <https://www.hrw.org/report/2020/09/10/video-unavailable/social-mediaplatforms-remove-evidence-war-crimes> (última consulta: 18-09-23).

²¹ JORIS VAN HOBOKEN, J., *The Proposed EU Terrorism Content Regulation: Analysis and Recommendations with Respect to Freedom of Expression Implications*, Transatlantic Working Group, 2019, p. 7, disponible en https://www.ivir.nl/publicaties/download/TERREG_FoE-ANALYSIS.pdf (última consulta: 18-09-23).

El Reglamento se aplica a todos los prestadores que ofrecen sus servicios en la UE independientemente de si están radicados en la misma o no, por lo tanto, tiene un efecto extraterritorial y un impacto global como todas las normas recientes de la UE que regulan cuestiones relativas a los intermediarios de Internet²². Se ha criticado además que podría ser usado como una inspiración por regímenes autoritarios para adoptar normas similares y provocar mayor censura en Internet²³.

El objetivo principal de la norma es obligar a los prestadores a retirar los contenidos terroristas o bloquear el acceso a ellos en el plazo de una hora desde la recepción de una orden de retirada emitida por una autoridad competente de un Estado miembro. Se trata de una obligación muy discutida porque se aplica a todos los proveedores independientemente de su tamaño, lo cual puede resultar desproporcionado porque requerirá un mecanismo que pueda funcionar todos los días a todas las horas (24/7). Esta idea que ya formaba parte de la propuesta de la Comisión se matizó en el texto definitivo levemente porque la autoridad competente debe informar al prestador con doce horas de antelación sobre la primera orden de retirada, salvo en casos de urgencia. Además, en caso de que existan razones técnicas u operativas objetivamente justificables que impidan el cumplimiento de la orden de retirada, se suspenderá el plazo.

Keller, que trabajó para Google en estos temas, explica que muchas de las empresas más grandes hacen un esfuerzo real para identificar solicitudes de mala fe o erróneas, con el fin de evitar eliminar el contenido legal del usuario.²⁴ Pero los errores son inevitables dado el gran volumen de solicitudes y el hecho de que las empresas de tecnología simplemente no conocen el contexto y los hechos subyacentes para la mayoría de las disputas. Desde

²² ANA GASCÓN MARCÉN, «El Reglamento General de Protección de Datos como modelo de las recientes propuestas de legislación digital europea», *Cuadernos de Derecho Transnacional*, vol. 13, t. 2, 2021.

²³ DIA KAYALI, «European «terrorist content» proposal is dangerous for human rights globally», *Witness*, 6-12-2018, disponible en <https://blog.witness.org/2018/12/european-terrorist-content-proposal-dangerous-human-rights-globally/> (última consulta: 18-09-23).

²⁴ DAPHNE KELLER, «Empirical evidence of over-removal by internet companies under intermediary liability laws: an updated list», *Center for Internet and Society*, 8-2-2-2021, disponible en http://cyberlaw.stanford.edu/blog/2021/02/empirical-evidence-over-removal-internet-companies-under-intermediary-liability-laws_ (última consulta: 18-09-23).

un punto de vista práctico explica que la ruta más fácil, barata y que evita riesgos para cualquier intermediario es simplemente procesar una solicitud de eliminación sin cuestionar su validez. Una empresa que adopta un enfoque de «en caso de duda, elimínalo» a las solicitudes puede ser simplemente un actor económico racional. Las pequeñas empresas sin el presupuesto para contratar abogados, o aquellas que operan en sistemas legales con protecciones poco claras, pueden ser particularmente propensas a tomar esta ruta. Además, esta regla aumenta la ventaja competitiva de las plataformas consolidadas con posibles efectos sobre la competencia²⁵.

Al ser tan reducido el tiempo que se da para retirar o bloquear los contenidos sumado a las cuantiosas sanciones que puede conllevar no hacerlo, en la práctica se entiende que esto llevara a los intermediarios a retirar todo el contenido que les sea notificado, sin plantearse si puede ser lícito, es decir, retirar el contenido por defecto para evitar cualquier responsabilidad.

También se ha criticado que este proceso se centra principalmente en las salvaguardias *ex post*, por lo que el potencial de bloqueos indebidos y abusos políticos es demasiado grande para proteger adecuadamente la libertad de expresión y comunicación, así como para cumplir con la prueba de proporcionalidad establecida por el derecho europeo e internacional de derechos humanos²⁶.

Por otra parte, se ha criticado que las órdenes pudieran dirigirse directamente a un intermediario situado en otro Estado miembro sin pasar por las autoridades de ese Estado, es decir, su carácter transfronterizo²⁷. Esto

²⁵ GIOVANNI DE GREGORIO, «Fighting Terrorism Online: Censorship, Platforms and Freedom of Expression across the Atlantic», *Virtual freedoms, Terrorism and the Law*, Routledge, 2021, pp. 95-117.

²⁶ EDRI ET AL., *How-to: Fundamental rights-compliant removal orders in the Terrorist Content Online Regulation*, 28-10-2020, disponible en https://edri.org/wp-content/uploads/2020/11/CivilSocietyBriefing_TCORemovalOrders_Oct2020.pdf (última consulta: 18-09-23).

²⁷ *Open letter on behalf of civil society groups regarding the proposal for a Regulation on Terrorist Content Online*, 9-11-2020, disponible en https://edri.org/wp-content/uploads/2020/11/TERREG_Openletter_Liberties.pdf (última consulta: 18-09-23); ALEKSANDRA KUCZERAWY, *The proposed Regulation...* cit.; y LIDIA DUTKIEWICZ y NOÉMIE KRACK., «All eyes riveted on the trilogue closed doors of the Proposal for a Regulation on preventing the dissemination of terrorist content online [Part I]», *KU Leuven CiTIP Blog*, 24-11-2020, disponible en <https://www.law.kuleuven.be/citip/blog/all-eyes-riveted-on-the-trilogue-closed-doors-of-the-proposal-for-a-regulation-on-preventing-the-dissemination-of-terrorist-content-online-part-i/> (última consulta: 18-09-23).

parece ser una tendencia reciente pues la misma lógica se aplicó en la propuesta de la Comisión Europea de órdenes europeas de entrega y conservación de pruebas electrónicas a efectos de enjuiciamiento penal. Si bien el carácter transfronterizo de las mismas sin involucrar al Estado en el que esté situado el intermediario destinatario también fue muy controvertido, como se explicará *infra*.

En el texto definitivo del Reglamento se incluyó un artículo sobre los procedimientos para las órdenes de retirada transfronterizas para permitir a la autoridad competente del Estado miembro en el que esté establecido, o tenga su representante legal, el prestador examinar la orden de retirada para determinar si contiene o no violaciones manifiestas o graves de los derechos fundamentales o del Reglamento. Lo mismo ha ocurrido con las órdenes de producción y entrega de pruebas electrónicas, puesto que se notificará al Estado donde esté localizado el intermediario.

Además, los prestadores y los proveedores de contenidos tienen derecho a solicitar una revisión de la orden de retirada por parte de dicha autoridad, que estará obligada a llevar a cabo el examen y exponer sus conclusiones en una decisión. Cuando el examen conduzca a la constatación de infracciones manifiestas o graves, la orden de retirada dejará de tener efectos jurídicos y el prestador ya no estará obligado a retirar el material y, en principio, deberá restablecerlo.

Por otra parte, la norma busca la puesta en práctica de medidas proactivas por parte de los prestadores para luchar contra los contenidos terroristas. Los prestadores deberán tomar medidas proactivas para proteger sus servicios frente a la difusión de contenidos terroristas. Las medidas serán eficaces y proporcionadas, teniendo en cuenta el riesgo y el nivel de exposición a contenidos terroristas, los derechos fundamentales de los usuarios y la importancia capital de la libertad de expresión y de información en una sociedad abierta y democrática.

Cuando un prestador hubiera recibido una orden de retirada debería presentar un informe sobre las medidas proactivas específicas que hubiera tomado, incluidas las que hubieran supuesto el uso de instrumentos automatizados, con el fin de: evitar que vuelvan a subirse contenidos que hayan sido retirados o cuyo acceso haya sido bloqueado previamente por considerarse que se trataba de contenidos terroristas; y detectar e identificar los contenidos terroristas y retirarlos o bloquear el acceso a ellos con celeridad. Si la autoridad

competente considerase que las medidas notificadas fueran insuficientes para atenuar y gestionar el riesgo y el nivel de exposición, podría solicitar al prestador que tomara medidas adicionales. Estas obligaciones se aplican únicamente a aquellos prestadores que la autoridad competente haya constatado que están expuestos a contenidos terroristas. Aunque las autoridades competentes pueden exigir a los prestadores que adopten medidas adicionales, la elección de las mismas corresponderá a los prestadores, a quienes no podrá obligarse a utilizar herramientas automatizadas.

Los prestadores establecerán en sus términos y condiciones su política destinada a evitar la difusión de contenidos terroristas, incluida, cuando proceda, una explicación sustanciosa del funcionamiento de las medidas proactivas, entre ellas el uso de instrumentos automatizados. Esta es una medida de transparencia interesante porque hasta ahora existía una información muy limitada de cómo funcionaban porque estaban cubiertos por una cierta opacidad. Se trata de una medida que sigue una reciente tendencia europea en áreas conexas que buscan una mayor transparencia de los procesos algorítmicos como la recogida en el Reglamento sobre servicios de intermediación en línea de 2019 y la *Digital Services Act* (DSA) de 2022.

Otra medida relevante a favor de la transparencia es que los prestadores publicarán informes anuales sobre las actuaciones llevadas a cabo contra la difusión de contenidos terroristas. Las autoridades estatales también deberían elaborar informes anuales que hicieran públicos donde apareciera información cualitativa y cuantitativa sobre las ordenes de retirada, sobre cuántas se presentaban, a qué intermediarios iban dirigidas, cuántas terminaban con una condena judicial, cuántas eran recurridas, etc. Esto ayudaría a tener una visión mucho más completa de la cuestión de cara a futuras medidas tanto legislativas como de otro tipo, además de mejorar el control y la rendición de cuentas de las autoridades públicas²⁸.

Cuando los prestadores usen instrumentos automatizados de conformidad con el Reglamento aplicarán garantías eficaces y adecuadas para asegurar que

²⁸ Véase TECH AGAINST TERRORISM, *Government Transparency Reporting on Online Counterterrorism Efforts*, disponible en <https://static1.squarespace.com/static/609d273957ee294d03d8dadf/t/60fe84736b5d5b2618fcd95/1627292788720/TAT+Guidelines+-+Government+transparency+reporting+on+online+counterterrorism+efforts.pdf> (última consulta: 18-09-23).

las decisiones tomadas, en particular las decisiones de retirar los contenidos o bloquear el acceso a ellos, sean precisas y bien fundamentadas. Dichas garantías consistirán en la supervisión y verificaciones por personas, cuando proceda y, en cualquier caso, cuando se precise una evaluación detallada del contexto pertinente para determinar si los contenidos deben considerarse contenidos terroristas o no. Los prestadores establecerán mecanismos eficaces y accesibles que permitan a los usuarios cuyos contenidos hayan sido retirados o hayan visto bloqueado su acceso como consecuencia de un requerimiento o de medidas proactivas (no en el caso de una orden de retirada) una reclamación contra la actuación del prestador en la que se solicite el restablecimiento del contenido. Los prestadores deben examinar rápidamente todas las reclamaciones que reciban y restablecer el contenido sin demora indebida cuando la retirada o el bloqueo del acceso no estuviesen justificado. Informarán al reclamante sobre el resultado del examen. Se trata de medidas positivas para asegurar los derechos de los usuarios que no estaban reguladas, y que van en la línea también de lo establecido en la DSA para todo tipo de moderación de contenidos.

Cuando los prestadores hayan retirado contenidos terroristas o bloqueado el acceso a ellos, pondrán a disposición del proveedor de contenidos información sobre la retirada o el bloqueo, siempre que esto no vaya en contra de la seguridad pública. A petición del proveedor de contenidos, el prestador informará a este sobre los motivos de la retirada o del bloqueo y las posibilidades de impugnación de la decisión. No obstante, Kuczerawy apunta que no se dan detalles sobre ese proceso de impugnación y simplemente apuntar su existencia no es suficiente²⁹. Según van Hoboken, la falta de revisión judicial y mecanismos de apelación efectivos para las órdenes de retirada es uno de los aspectos de la propuesta que más claramente viola la jurisprudencia establecida en materia de libertad de expresión³⁰.

Cuando los prestadores tengan conocimiento de cualquier indicio de delitos de terrorismo, informarán rápidamente a las autoridades competentes para investigar y enjuiciar infracciones penales en el Estado miembro correspondiente. Los prestadores podrán, en caso de duda, transmitir esa información a Europól para que se le dé el curso adecuado.

²⁹ ALEKSANDRA KUCZERAWY, *The proposed Regulation...* cit.

³⁰ JORIS VAN HOBOKEN, J., *The Proposed EU Terrorism...* cit., p. 8.

Volviendo a las medidas proactivas éstas deberán ser proporcionadas, teniendo en cuenta el riesgo y el nivel de exposición a contenidos terroristas. Es importante la inclusión de este inciso diferenciando el nivel de riesgo de unos proveedores y otros, pero se puede ver que se trataría en muchos casos de utilizar filtros automáticos. Kuczerawy argumenta que las medidas proactivas impuestas por las autoridades competentes podrían dar lugar a obligaciones generales de seguimiento prohibidas por el Derecho de la UE³¹, en concreto actualmente la DSA.

Normalmente, se aplicarán dos tipos de filtros³². El primer tipo funciona con *hashes* y compara los vídeos subidos con una base de datos de contenido que haya sido clasificado como terrorista. A raíz, de la insistencia de mayores esfuerzos en esta área por parte de la Comisión Europea, Google, Facebook, Twitter y Microsoft crearon en 2017 la *Global Internet Forum to Counter Terrorism* (GIFCT) que creó esa base de datos de *hashes* centralizada para coordinar sus esfuerzos y que presta sus servicios a prestadores más pequeños. Esta entidad tenía un fuerte impacto en la libertad de expresión en línea y, sin embargo, su funcionamiento era tremendamente opaco³³. Posteriormente se independizó de sus creadores convirtiéndose en una ONG que busca

³¹ ALEKSANDRA KUCZERAWY, *The proposed Regulation...* cit.

³² LIDIA DUTKIEWICZ y NOÉMIE KRACK, «How to notice without looking: the ‘algorithmization’ of terrorist content moderation in the Proposal for a Regulation on preventing the dissemination of terrorist content online [Part II]», *KU Leuven CiTIP Blog*, 25-11-2020, disponible en <https://www.law.kuleuven.be/citip/blog/how-to-notice-without-looking-the-algorithmization-of-terrorist-content-moderation-in-the-proposal-for-a-regulation-on-preventing-the-dissemination-of-terrorist-content-online-part-ii/> (última consulta: 18-09-23). Para un estudio sobre cómo funcionan estos filtros y sus problemas véase CAREY SHENKMAN, DHANARAJ THAKUR y EMMA LLANSÓ, «¿Do You See What I See? *Capabilities and Limits of Automated Multimedia Content Analysis*», Center for Democracy & Technology, 2021, disponible en <https://cdt.org/insights/do-you-see-what-i-see-capabilities-and-limits-of-automated-multimedia-content-analysis/> (última consulta: 18-09-23).

³³ BRITTAN HELLER, *Combating Terrorist-Related Content through AI and Information Sharing*, Transatlantic Working Group, 2019, disponible en https://www.ivir.nl/publicaties/download/Hash_sharing_Heller_April_2019.pdf (última consulta: 18-09-23); EVELYN DOUEK, *The Rise of Content Cartels*, Knight First Amendment Institute, 2020, disponible en <https://knightcolumbia.org/content/the-rise-of-content-cartels> (última consulta: 18-09-23); y EMMA LLANSÓ, «Platforms Want Centralized Censorship. That Should Scare You», *Wired*, 18-4-2019, disponible en <https://www.wired.com/story/platforms-centralized-censorship/> (última consulta: 18-09-23).

tener contacto con más diversas partes interesadas y en 2021 fue objeto de una evaluación de impacto de derechos humanos³⁴.

Las Relatoras de Naciones Unidas mostraron su preocupación respecto a este punto porque, si bien entendían el uso de *hashes* para identificar imágenes de abuso sexual infantil, consideraban que su aplicación al contenido «extremista», que generalmente requiere una evaluación del contexto, era difícil de lograr sin la evaluación humana. Además, explicaban que, incluso si una imagen en particular es ilegal cuando se usa con la intención de incitar a la comisión de actos de terrorismo, su uso puede ser legítimo con fines periodísticos³⁵.

El segundo tipo de filtros busca detectar contenido nuevo a través de programas de inteligencia artificial, por ejemplo, de procesamiento del lenguaje natural. El problema es que estos mecanismos no tienen capacidad para detectar la ironía o la sátira, esto es especialmente complejo cuando hablamos de «contenidos terroristas» y afectan de manera desproporcionada a grupos vulnerables³⁶. Cuando YouTube se vio obligado a reforzar sus esfuerzos para luchar contra el contenido terrorista y aplicó para ello un programa de inteligencia artificial borró miles de videos del *Syrian Archive* que buscaban atestiguar y servir como prueba de las atrocidades cometidas en la guerra de Siria³⁷. Esto llevó a varias ONG a pedir al Parlamento Europeo que no fomentara el uso de medidas proactivas/filtros automáticos de la propuesta porque podían llevar a la desaparición de pruebas relevantes para

³⁴ BSR, *Human Rights Assessment. Global Internet Forum to Counter Terrorism*. 2021, disponible en <https://www.bsr.org/reports/BSR-GIFCT-Report.pdf> (última consulta: 18-09-23).

³⁵ *Carta de Irene Khan y Fionnuala Ni Aoláin de 3 de noviembre de 2020*. OL OTH 73/2020, disponible en <https://spcommreports.ohchr.org/TMResultsBase/DownloadPublicCommunicationFile?gId=25661> (última consulta: 18-09-23).

³⁶ Véase NATASHA DUARTE, EMMA LLANSO, E. Y ANNA LOUR, *Mixed Messages? The Limits of Automated Social Media*, Center for Democracy & Technology, 2017; y FINCK, M., *Artificial intelligence and online hate speech*, Centre on Regulation in Europe, 2019.

³⁷ KATE O'FLAHERTY, «YouTube keeps deleting evidence of Syrian chemical weapon attacks», *Wired*, 26-06-2018, disponible en <https://www.wired.co.uk/article/chemical-weapons-in-syria-youtube-algorithm-delete-video> (última consulta: 18-09-23); y HADI AL KHATIB y DIA KAYYALI, «YouTube Is Erasing History. Under pressure to remove «extremist content», platforms are purging vital human rights evidence», *The New York Times*, 23-10-2019, disponible en <https://www.nytimes.com/2019/10/23/opinion/syria-youtube-content-moderation.html> (última consulta: 18-09-23).

futuras investigaciones o para fines educativos³⁸. Y es que el uso de filtros puede vulnerar la libertad de expresión, pero también el derecho a la información, la privacidad, la protección de datos y la igualdad.

Cada Estado debe designar las autoridades competentes para emitir órdenes de retirada de contenidos. Se ha criticado que los Estados puedan elegir autoridades tanto administrativas, como policiales y judiciales. Si bien los Estados deben asegurar que éstas no soliciten ni reciban instrucciones (es decir, sean independientes) y actúen de manera objetiva y no discriminatoria, garantizando el pleno respeto de los derechos fundamentales. Teruel argumentó al respecto que el Reglamento daría lugar «a un indudable efecto disuasorio en el ejercicio de las libertades sólo mitigable con el más amplio reconocimiento de las debidas garantías, entre las cuales entiendo que debe reconocerse que sea una autoridad judicial la que decida»³⁹. En el caso de España la autoridad competente es el Centro de Inteligencia contra el Terrorismo y el Crimen Organizado (CITCO) que depende de la Secretaría de Estado de Seguridad.

Respecto a las sanciones, se ha incluido la posibilidad explícita de que los Estados decidan imponerlas en casos concretos, teniendo en cuenta circunstancias como la naturaleza y el tamaño del prestador de que se trate, el grado de culpa por la infracción y las medidas técnicas y organizativas que haya podido adoptar para garantizar el cumplimiento de los requisitos del Reglamento.

Varias ONG especializadas en la defensa de los derechos humanos de los usuarios de Internet (como *Access Now* o Article 19) pidieron sin éxito a los miembros del Parlamento Europeo que votaran contra el Reglamento por incentivar el uso por parte de las plataformas en línea de herramientas automatizadas de moderación de contenidos, como los filtros, la severa falta de control judicial independiente y por permitir a los Estados emitir órdenes transfronterizas de retirada sin ningún control⁴⁰.

En ese sentido, Scheinin, que fue primer relator especial de las Naciones Unidas sobre derechos humanos y lucha contra el terrorismo, reaccionó a

³⁸ *NGOs Joint letter*, 4-12-2019, disponible en <https://cdt.org/wp-content/uploads/2019/02/Civil-Society-Letter-to-European-Parliament-on-Terrorism-Database.pdf> (última consulta: 18-09-23).

³⁹ GERMÁN MANUEL TERUEL LOZANO, «Una lectura garantista...», cit.

⁴⁰ *Joint letter to members of the European Parliament*, 2021, disponible en https://edri.org/wp-content/uploads/2021/04/MEP_TERREG_Letter_EN_78.pdf.

su aprobación diciendo que se trataba de una ley mal redactada que lo más probable es que causase problemas reales en lugar de convertirse en una pieza más del antiterrorismo meramente simbólico⁴¹. *Tech Againsts Terrorism* temía que el Reglamento haría poco para lograr su propósito de combatir el uso terrorista de Internet y corría el riesgo de dañar la innovación y la competencia en el proceso⁴².

No obstante, otros se han mostrado más positivos con la norma, Teruel señaló que ofrecía una respuesta ponderada que trataba de equilibrar las exigencias de seguridad derivadas de la lucha contra el terrorismo con las exigencias garantistas y el respeto de los derechos fundamentales afectados, especialmente las libertades de expresión y de información (aunque con margen de mejora)⁴³. Mientras que para De Gregorio era un ejemplo del nuevo enfoque constitucional digital europeo con el objetivo de proteger los derechos fundamentales y los valores democráticos al tiempo que limitaba el poder privado de las plataformas en línea⁴⁴.

La cuestión es saber si el Reglamento cuenta con las suficientes garantías de derechos conforme a la Carta de los Derechos Fundamentales de la UE (CDFUE) y si pasaría el test de una posible cuestión prejudicial de validez ante el Tribunal de Justicia de la UE (TJUE). En ese sentido, el artículo de la Directiva que moderniza la protección de los derechos de autor que fomenta el uso de filtros para evitar la responsabilidad de los prestadores de servicios para compartir contenidos en línea fue recurrido ante este Tribunal por Polonia por vulnerar la libertad de expresión. El Tribunal concluyó que el artículo era compatible con el derecho de la UE, no obstante, subrayó la necesidad de salvaguardias suficientes para los usuarios y de evitar que se

⁴¹ <https://twitter.com/MartinScheinin/status/1387767514688524302> (última consulta: 18-09-23).

⁴² TECH AGAINST TERRORISM, *The Online Regulation Series. The Handbook*, 2021, p. 101, disponible en <https://www.techagainstterrorism.org/wp-content/uploads/2021/07/Tech-Against-Terrorism-%E2%80%93-The-Online-Regulation-Series-%E2%80%93-The-Handbook-2021.pdf> (última consulta: 18-09-23).

⁴³ GERMÁN MANUEL TERUEL LOZANO, «Una lectura garantista...», cit.

⁴⁴ GIOVANNI DE GREGORIO, «The rise of digital constitutionalism in the European Union», *International Journal of Constitutional Law*, vol. 19, t. 1, 2021, pp. 41–70, disponible en <https://doi.org/10.1093/icon/moab001> (última consulta: 18-09-23).

bloquearán o filtrarán contenidos lícitos,⁴⁵ lo cual puede ser más complejo en el caso de ciertos contenidos que pueden estar en el límite de poder ser considerados terroristas que cuando hablamos de contenido protegido por derechos de autor. Si bien la protección de los derechos de autor y la lucha contra el terrorismo no son intercambiables muchas de sus aseveraciones podrían aplicarse también a la materia de este capítulo.

En 2020, Francia adoptó una Ley destinada a combatir los contenidos de odio en Internet (*Loi visant à lutter contre les contenus haineux sur internet* o *Loi Avia*) que tenía algunos elementos en común con el Reglamento. La Ley fue posteriormente anulada parcialmente por el Consejo Constitucional francés.⁴⁶ En particular el Consejo anuló el inciso I del artículo 1 de la Ley que disponía que la autoridad administrativa podría solicitar los proveedores de un servicio de comunicación en línea eliminar cierto contenido terrorista en una hora y si no lo hacían podían ser objeto de una sanción de un año de prisión y multa de 250.000 euros. El Consejo consideró que la medida no era adecuada, necesaria y proporcionada al objetivo legítimo perseguido.

Por último, en 2022, la UE adoptó la DSA que mantenía los principios de la Directiva de Comercio Electrónico, pero matizaba algunas cuestiones y creaba obligaciones de diligencia debida para los intermediarios de Internet.⁴⁷ Ésta si bien no se dedica específicamente a la lucha contra el terrorismo establece normas armonizadas sobre la prestación de servicios intermediarios

⁴⁵ STJUE de 26 de abril de 2022, República de Polonia c. Parlamento Europeo, Consejo de la Unión Europea, as. C-401/19.

⁴⁶ Consejo Constitucional, *Décision n° 2020-801 DC du 18 juin 2020*.

⁴⁷ Reglamento (UE) 2022/2065 del Parlamento Europeo y del Consejo de 19 de octubre de 2022 relativo a un mercado único de servicios digitales y por el que se modifica la Directiva 2000/31/CE (Reglamento de Servicios Digitales), DOUE L 277 de 27.10.2022, p. 1/102. Véase ANA GASCÓN MARCÉN, «La responsabilidad de los intermediarios de Internet en la Unión Europea: iniciativas recientes y perspectivas de futuro», *Desafíos jurídicos ante la integración digital: aspectos europeos e internacionales*, Aranzadi, 2021, pp. 133-160; y JOSÉ JUAN CASTELLÓ PASTOR, «Nuevo régimen de responsabilidad de los servicios digitales que actúan como intermediarios a la luz de la propuesta de Reglamento relativo a un mercado único de servicios digitales», *Desafíos jurídicos ante la integración digital: aspectos europeos e internacionales*, Aranzadi, 2021, pp. 37-76; y JONATÁN CRUZ ÁNGELES, «Las obligaciones jurídico-comunitarias de las grandes plataformas proveedoras de servicios digitales en la era del metaverso». *Cuadernos de Derecho Transnacional*, 14(2), 2022, pp. 294-318. <https://doi.org/10.20318/cdt.2022.7186>

en el mercado interior y recoge también normas sobre responsabilidad y transparencia de los mismos. Se crean obligaciones adicionales de gestión de riesgos sistémicos para plataformas y motores de búsqueda en línea de muy gran tamaño.⁴⁸ Estas disposiciones tienen implicaciones para la lucha contra los contenidos terroristas a través de las evaluaciones de riesgos que deben analizar cualquier efecto negativo real o previsible sobre la seguridad pública, las medidas para su mitigación y el mecanismo de respuesta a crisis que está pensado, entre otras circunstancias, para que pueda aplicarse en casos de terrorismo. Además, se establece la obligación para los prestadores de comunicar las autoridades policiales o judiciales de los Estados miembros de cualquier sospecha cuando tenga conocimiento de cualquier información que les haga pensar que se ha cometido, se está cometiendo o es probable que se cometa un delito que implique una amenaza para la vida o la seguridad de una o más personas, como es el caso de los atentados terroristas.

La DSA se aplica también a los prestadores en la medida en que el Reglamento para la prevención de la difusión de contenidos terroristas en línea no contengan disposiciones de carácter más específico que les sean aplicables, es decir este último actúa como *lex specialis*.

Es interesante comparar el régimen europeo con el de los Estados Unidos, donde están situados muchos de los grandes proveedores de Internet y que es mucho más permisivo puesto que la sección 230 de la *Communications Decency Act* exime de responsabilidad a los proveedores de servicios de Internet por el contenido publicado por terceros⁴⁹, si bien existe un gran debate en Estados Unidos sobre el mismo. Recientemente dos casos han sido decididos por el Tribunal Supremo de Estados Unidos respecto a actos terroristas en los que los demandantes pretendían que se matizara la interpretación de este artículo y que argumentaron que Twitter y Google (como propietario de YouTube) debían considerarse como cómplices o conspiradores necesarios de las actividades del ISIS, pero no han prosperado en sus pretensiones.⁵⁰

⁴⁸ Se trata de aquellas que tengan un promedio mensual de destinatarios del servicio activos en la UE igual o superior a cuarenta y cinco millones.

⁴⁹ Véase JOSÉ JUAN CASTELLÓ PASTOR, «Exoneración de responsabilidad de los prestadores de servicios de la información en la sección 230 de la Communications Decency Act estadounidense», *Revista Aranzadi de derecho y nuevas tecnologías*, n.º. 39, 2015, pp. 175-194.

3. Pruebas electrónicas

Según la Comisión Europea, las pruebas electrónicas en cualquiera de sus formas son relevantes en alrededor del 85% de las investigaciones penales.⁵¹ En muchos casos, en las primeras fases de las investigaciones se recaban datos de las operadoras de comunicaciones, de las compañías telefónicas tradicionales en relación a las llamadas de teléfono, pero también cada vez más de los proveedores de servicios de Internet para saber con quién se ha estado en contacto, qué páginas se han consultado y contenido compartido, qué se ha dicho en los foros y redes sociales, etc. Esta información está en manos de los intermediarios de Internet. En este apartado examinaremos los deberes de conservación de datos a los que se someten algunos de ellos y las nuevas órdenes europeas de entrega y conservación de pruebas electrónicas a efectos de enjuiciamiento penal.

3.1 Conservación de datos

Para garantizar que los datos estuvieran disponibles con fines de investigación, detección y enjuiciamiento de delitos graves, la Directiva europea de conservación de datos⁵² establecía que los servicios de comunicaciones electrónicas de acceso público o de una red pública de comunicaciones

⁵⁰ Véase Decisión del Tribunal Supremo de los Estados Unidos de 18 de mayo de 2023, *Twitter, INC. v. Taamneh et al.* C No. 21-1496 (https://www.supremecourt.gov/opinions/22pdf/21-1496_d18f.pdf última consulta: 18-09-23) y Decisión del Tribunal Supremo de los Estados Unidos de 18 de mayo de 2023, *Reynaldo Gonzalez, et al., petitioners v. Google LLC*, No. 21-1333 (https://www.supremecourt.gov/opinions/22pdf/21-1496_d18f.pdf última consulta: 18-09-23).

⁵¹ Comisión Europea, *Impact Assessment accompanying the document Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters and Proposal for a Directive of the European Parliament and of the Council laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings*, SWD/2018/118 final – 2018/0108 (COD), 17 de abril de 2018, p. 14.

⁵² Directiva 2006/24/CE del Parlamento Europeo y del Consejo, de 15 de marzo de 2006, sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones y por la que se modifica la Directiva 2002/58/CE, DOUE L 105 de 13.4.2006, pp. 54-63.

debían conservar toda una serie de datos relativos a sus usuarios como su nombre, destinatario de las comunicaciones, la fecha y hora del comienzo y fin de las mismas, etc., es decir, no el contenido de las comunicaciones sino sus metadatos, por un tiempo no inferior a seis meses ni superior a dos años a partir de la fecha de la comunicación. Esto convertía a los intermediarios de Internet en una especie de intermediarios de la vigilancia (*surveillance intermediaries*) al servicio del Estado para poder acceder a los datos.⁵³ Brown y Korf consideraron que los derechos a la privacidad y a la no discriminación que son fundamentales en el marco jurídico europeo estaban siendo cuestionados por el aumento de la vigilancia y la elaboración de perfiles de los sospechosos de terrorismo. Argumentaron que su naturaleza desproporcionada era problemática para la democracia y el estado de derecho.⁵⁴

A raíz de una cuestión prejudicial presentada ante el TJUE, éste invalidó la Directiva.⁵⁵ El TJUE consideró que las obligaciones impuestas por la Directiva constituían una injerencia en el respeto de la vida privada y el respeto de la vida privada derechos garantizados por los artículos 7 y 8 respectivamente de la CDFUE. Esta injerencia resultaba de gran magnitud y debía considerarse especialmente grave, porque los metadatos pueden permitir extraer conclusiones muy precisas sobre la vida privada de las personas, como los hábitos de la vida cotidiana, los lugares de residencia permanentes o temporales, los desplazamientos diarios, las actividades realizadas, las relaciones sociales y los medios sociales que frecuentan.

El TJUE reconoció que la lucha contra la delincuencia grave, especialmente contra el terrorismo, reviste una importancia primordial para garantizar la seguridad pública y su eficacia puede depender en gran medida de la utilización

⁵³ Sander explica que los intermediarios ejercen esta función junto con la de *surveillance principals* al basar sus propios modelos de negocio extractivitas en la explotación de los datos. BARRIE SANDER, «Democratic Disruption in the Age of Social Media: Between Marketized and Structural Conceptions of Human Rights Law». *European Journal of International Law*. 32 (1), 2021 <https://doi.org/10.1093/ejil/chab022> (última consulta: 18-09-23).

⁵⁴ IAN BROWN y DOUWE KORFE, «Terrorism and the proportionality of internet surveillance», *European Journal of Criminology*, vol. 6, nº 2, 2009, pp. 119-134.

⁵⁵ STJUE, *Digital Rights Ireland Ltd c. Minister for Communications, Marine and Natural Resources, Minister for Justice, Equality and Law Reform, Commissioner of the Garda Síochána, Irlanda y The Attorney General*; y *Kärntner Landesregierung, Michael Seitlinger, Christof Tschohl y otros*, as. ac. C-293/12 y C-594/12, 8 de abril de 2014.

de técnicas modernas de investigación. Sin embargo, este objetivo de interés general no podía por sí solo justificar que una medida de conservación de datos como la establecida por la Directiva se considerase necesaria a los efectos de dicha lucha.

La Directiva era aplicable a todos los medios de comunicación electrónica, cuyo uso está muy extendido y que tienen una importancia creciente en la vida cotidiana de las personas, y comprendía a todos los abonados y usuarios registrados, por lo que constituía una injerencia en los derechos fundamentales de prácticamente toda la población europea. Así, la Directiva abarcaba de manera generalizada a todas las personas, medios de comunicación electrónica y datos relativos al tráfico sin que se estableciera ninguna diferenciación, limitación o excepción en función del objetivo de lucha contra los delitos graves. La Directiva además no fijaba ningún criterio objetivo que permitiera delimitar el acceso de las autoridades nacionales competentes a los datos y su utilización posterior con fines de prevención, detección o enjuiciamiento de delitos que pudieran considerarse suficientemente graves para justificar tal injerencia. La Directiva no precisaba las condiciones materiales y de procedimiento correspondientes al acceso de las autoridades nacionales competentes a los datos y su utilización posterior, y prescribía la conservación de los datos durante un período mínimo de seis meses sin que se estableciera ninguna distinción entre las categorías de datos en función de su posible utilidad para el objetivo perseguido o de las personas afectadas. La Directiva ni siquiera contenía garantías suficientes que permitieran asegurar una protección eficaz de los datos conservados contra los riesgos de abuso y de acceso y utilización ilícitos. Por todo ello, el TJUE consideró que el legislador había sobrepasado los límites que exigía el respeto del principio de proporcionalidad.

La doctrina en general aplaudió esta sentencia al considerar que el TJUE había actuado como el garante de los derechos en la UE⁵⁶ y que había dado una lección al legislador europeo en materia de privacidad y protección de datos.⁵⁷ Cabe añadir que este tipo de vigilancia según Shahbaz

⁵⁶ María Isabel GONZÁLEZ PASCUAL, «EL TJUE como garante de los derechos en la UE a la luz de la sentencia *Digital Rights Ireland*», *Revista de Derecho Comunitario Europeo*, Año 18, nº 49, 2014, pp. 943-971.

⁵⁷ MARIE-PIERRE GRANGER y KRISTINA IRION, «The Court of Justice and the Data Retention

y Funk no sólo plantea riesgos para la privacidad sino que puede exacerbar la discriminación, restringir la libertad de expresión, asociación y reunión y socavar el debido proceso.⁵⁸ Murray y Fussey han sostenido, analizando la cuestión desde la perspectiva de derechos humanos, que los cálculos de utilidad y daño pueden ocultar la naturaleza compleja de las prácticas de vigilancia digital contemporáneas, haciendo que los enfoques actuales de la prueba de «necesidad» sean problemáticos. En su opinión, el análisis de los daños relacionados con la vigilancia debe extenderse más allá de las implicaciones de privacidad e incorporar efectos en toda la sociedad y es necesario desarrollar un enfoque más matizado para los datos de comunicaciones masivos.⁵⁹

La invalidación de la Directiva no supuso la desaparición de las normas nacionales de transposición. Algunos tribunales constitucionales las anularon, pero en muchos otros países siguieron aplicándose. Así, varias nuevas cuestiones prejudiciales sobre la aplicación de las mismas llegaron al TJUE que dictaminó en *Tele2* que el artículo 15 de la Directiva sobre la privacidad y las comunicaciones electrónicas, en relación con los artículos 7, 8, 11 y 52 CDFUE, debía interpretarse en el sentido de que se oponía a una normativa nacional que estableciera, con la finalidad de luchar contra la delincuencia, la conservación generalizada e indiferenciada de todos los datos de tráfico y de localización de todos los abonados y usuarios registrados en relación con todos los medios de comunicación electrónica. Además, se oponía a una normativa nacional que regulara el acceso de las autoridades nacionales competentes a los datos conservados sin supeditarlos a un control previo por un órgano jurisdiccional o una autoridad administrativa independiente.⁶⁰ El Tribunal aseveró que los metadatos

Directive in Digital Rights Ireland: Telling Off the EU Legislator and Teaching a Lesson in Privacy and Data Protection», *European Law Review*, nº 6, 2014, pp. 835-850.

⁵⁸ ADRIAN SHAHBAZ y ALLIE FUNK, *Freedom on the Net 2019: The Crisis of Social Media*, Freedom House, 2019 https://freedomhouse.org/sites/default/files/2019-11/11042019_Report_FH_FOTN_2019_final_Public_Download.pdf (última consulta: 18-09-23).

⁵⁹ DARAGH MURRAY y PETE FUSSEY, «Bulk Surveillance in the Digital Age: Rethinking the Human Rights Law Approach to Bulk Monitoring of Communications Data», *Israel Law Review*, vol. 52, nº 1, 2019, pp. 31-60.

⁶⁰ STJUE *Tele2 Sverige AB c.a Post-och telestyrelsen y Secretary of State for the Home Department c. Tom Watson y otros* as. ac. C-203/15 y C-698/15, 21 de diciembre de 2016.

permiten determinar «el perfil de las personas afectadas, información tan sensible, a la luz del respeto de la vida privada, como el propio contenido de las comunicaciones.»

A pesar de esta sentencia, las normas nacionales de transposición de la Directiva invalidada han seguido aplicándose con limitadas modificaciones. Esto hizo que surgieran nuevas dudas en su aplicación y validez por parte de los tribunales nacionales que plantearon más cuestiones al TJUE, de particular interés para la lucha antiterrorista fueron la sentencia de los asuntos acumulados C-511/18, C-512/18 y C-520/18, conocida como *La Quadrature du Net*⁶¹ (aunque había muchos más demandantes).

El elemento que distingue a esta sentencia de sus predecesoras es que las normas francesas y belgas tenían entre sus objetivos la salvaguarda de la seguridad nacional. La cuestión era saber si esta finalidad tenía alguna influencia en los estándares ya fijados por el TJUE en su jurisprudencia respecto a la conservación de datos para luchar contra la comisión de delitos.

El Tribunal reafirmó lo dicho en sus sentencias previas, pero con una importante matización, porque estableció que en situaciones en las que un Estado se enfrente a una amenaza grave para la seguridad nacional que resulte real y actual o previsible (como puede ser un atentado terrorista), puede imponer una conservación generalizada e indiferenciada de esos datos durante un período temporalmente limitado a lo estrictamente necesario, pero renovable en caso de persistencia de la amenaza. El TJUE abrió la puerta a una conservación generalizada que parecía estar prohibida por su anterior jurisprudencia, pero no de manera permanente, sino sólo cuando se den esos requisitos. Esto es así porque para el TJUE el objetivo de protección de la seguridad nacional puede justificar medidas que supongan injerencias en los derechos fundamentales más graves que las que podrían justificar

⁶¹ STJUE *La Quadrature du Net, French Data Network, Fédération des fournisseurs d'accès à Internet associatifs, Iqwan.net c. Premier ministre, Garde des Sceaux, Ministre de la Justice, Ministre de l'Intérieur y Ministre des Armées; y Ordre des barreaux francophones et germanophone, Académie Fiscale ASBL, UA, Liga voor Mensenrechten ASBL, Ligue des Droits de l'Homme ASBL, VZ, WY, XX y Conseil des ministres*, as. ac. C-511/18, C-512/18 y C-520/18, 6 de octubre de 2020. Véase ANA GASCÓN MARCÉN, «La sentencia *La Quadrature du Net* y el futuro de la normativa de conservación de datos», *Estudios sobre Jurisprudencia Europea: materiales del VI Encuentro anual del Centro español del European Law Institute*, Sepin, 2023, pp. 656-673.

otros objetivos, incluso la lucha contra los delitos graves. Vemos que el TJUE crea una categorización de los objetivos por su importancia.

No obstante, cabe señalar que el TJUE en la sentencia del mismo día en el caso *Privacy International*⁶² aclaró que el Derecho de la UE se opone a una normativa nacional que permite a una autoridad estatal obligar a los proveedores de servicios de comunicaciones electrónicas a realizar una transmisión generalizada e indiferenciada de datos de tráfico y de datos de localización a las agencias de seguridad e inteligencia con el fin de proteger la seguridad nacional. Es decir, los datos pueden conservarse, pero no transmitirse de manera generalizada, sólo se podrá acceder a los que sea necesario.

Por lo que se refiere a la prevención de amenazas graves contra la seguridad pública, un Estado puede disponer la conservación selectiva de dichos datos y su conservación rápida. Una injerencia de esta índole en los derechos fundamentales debe ir acompañada de garantías efectivas y ser controlada por un juez o una autoridad administrativa independiente. Así, vemos que en este caso la conservación generalizada queda prohibida en la lucha contra los delitos, incluso graves, pero surgen dudas sobre cómo se debería llevar a cabo en la práctica esa conservación selectiva apoyada por el TJUE.

Asimismo, para prevenir las amenazas graves contra la seguridad pública, un Estado puede realizar una conservación generalizada e indiferenciada de las direcciones IP atribuidas a la fuente de una comunicación cuando el período de conservación se limite a lo estrictamente necesario. Para luchar contra la delincuencia y proteger la seguridad pública, también se permite una conservación generalizada e indiferenciada de los datos relativos a la identidad civil de los usuarios de los medios de comunicaciones electrónicas, sin que ello se limite en este último caso a un plazo determinado. Así a la categorización de mayor o menor injerencia según los objetivos perseguidos se une otra categorización según el tipo de datos que según su sensibilidad también van a suponer una mayor o menor injerencia.

El TJUE además no sólo tuvo que pronunciarse en torno a los diferentes objetivos y tipos de datos conservados, sino a diferentes mecanismos como

⁶² STJUE *Privacy International c. Secretary of State for Foreign and Commonwealth Affairs, Secretary of State for the Home Department, Government Communications Headquarters, Security Service, Secret Intelligence Service*, C-623/17, 6 de octubre de 2020.

la conservación rápida, la recopilación en tiempo real y el análisis automatizado de los datos. El TJUE aceptó la posibilidad de utilizar los tres, pero con ciertas condiciones. Consideró que la Directiva de privacidad electrónica no se opone a una norma que permita el recurso a una conservación rápida (*quick freeze*) de los datos de que dispongan los proveedores cuando se produzcan situaciones en las que resulte necesario conservar dichos datos más allá de los plazos legales de conservación con el fin de esclarecer atentados contra la seguridad nacional, cuando ya hayan sido comprobados o cuando su existencia pueda sospecharse razonablemente. Además, consideró que la Directiva no se oponía a una normativa nacional que obliga a los proveedores a recurrir a la recopilación en tiempo real, en particular, de datos de tráfico y de localización, cuando se limite a las personas respecto de las que exista una razón válida para sospechar que están implicada en actividades terroristas y esté sometida a un control previo efectuado bien por un órgano jurisdiccional, bien por una entidad administrativa independiente, cuya decisión tenga carácter vinculante, que garantice que esa recopilación en tiempo real se autoriza solo en la medida en que sea estrictamente necesario. En caso de urgencia, el control deberá llevarse a cabo en breve plazo.

Respecto al análisis automatizado, se debe limitar a aquellas situaciones en las que un Estado se enfrenta a una amenaza grave para la seguridad nacional que resulte real y actual o previsible, pudiendo ser objeto el recurso a dicho análisis de un control efectivo, bien por un órgano jurisdiccional, bien por una entidad administrativa independiente, cuya decisión tenga carácter vinculante, que tenga por objeto comprobar la existencia de una situación que justifique dicha medida, así como el respecto de las condiciones y de las garantías que deben establecerse, como, por ejemplo, que cualquier resultado positivo obtenido gracias a un tratamiento automatizado debe reexaminarse individualmente por medios no automatizados antes de adoptar una medida individual que produzca efectos perjudiciales para las personas afectadas, o que los modelos y criterios preestablecidos a efectos del análisis no pueden basarse únicamente en datos sensibles como el origen racial o étnico, las opiniones políticas, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, la salud o a la sexualidad de una persona.

En este sentido, Sajfert ha criticado la sentencia por ser un importante paso atrás en la jurisprudencia del TJUE, al considerar que está compuesta por una serie de compromisos más políticos que judiciales y ejercicios para

salvar las apariencias.⁶³ En ese sentido es cierto que, aun reiterando lo dicho en *Digital Rights Ireland* y *Tele2*, el TJUE abre la puerta a la conservación generalizada e indiscriminada de todo tipo de metadatos en casos de seguridad nacional y de direcciones IP y datos relativos a la identidad civil para luchar contra la delincuencia y proteger la seguridad pública. Al final, el TJUE ha llegado a un compromiso visto lo sensible que es para los Estados la seguridad nacional y la lucha contra el terrorismo. Tracol ha afirmado que el TJUE en esta sentencia (y la de *Privacy International*) ha intentado cuadrar el círculo de la conservación de datos.⁶⁴

Los Estados miembros de la UE han resaltado en múltiples ocasiones la necesidad de la conservación de datos para proteger la seguridad nacional y luchar contra el crimen.⁶⁵ Eso ha llevado a que el impacto de las múltiples sentencias del TJUE en la normativa nacional sea limitado. España es un ejemplo más, puesto que sigue aplicando la Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones, con el apoyo del Tribunal Supremo a pesar de no cumplir los requisitos expuestos.⁶⁶

El Parlamento Europeo celebró una audiencia sobre el impacto de la sentencia *La Quadrature du Net* en 2021. En la misma, el Director-General Adjunto de la Dirección General de Migración y Asuntos de Interior de la Comisión Europea aseveró que ningún Estado miembros (ni siquiera los que habían empezado a ajustar su normativa) había encontrado la «fórmula mágica» para «cuadrar el círculo» y cumplir completamente con la jurisprudencia

⁶³ JURAJ SAJFERT, «Bulk data interception/retention judgments of the CJEU – A victory and a defeat for privacy», *European Law Blog*, 26/10/2020. <https://europeanlawblog.eu/2020/10/26/bulk-data-interception-retention-judgments-of-the-cjeu-a-victory-and-a-defeat-for-privacy/> (última consulta: 18-09-23).

⁶⁴ XAVIER TRACOL, «The two judgments of the European Court of Justice in the four cases of Privacy International, La Quadrature du Net and Others, French Data Network and Others and Ordre des Barreaux francophones et germanophone and Others: The Grand Chamber is trying hard to square the circle of data retention», *Computer Law & Security Review*, vol. 41. 2021.

⁶⁵ Véase, por ejemplo, Conclusiones del Consejo de la Unión Europea de 27 de mayo de 2019 sobre la conservación de datos a efectos de lucha contra la delincuencia, Doc. 9663/19.

⁶⁶ ANDONI POLO ROCA, «La regulación sobre la conservación de datos en el sector de las comunicaciones electrónicas o telecomunicaciones: estado de la cuestión», *IDP: Revista d'Internet, dret i política* 33, 2021.

del TJUE y al mismo tiempo garantizar el acceso de las autoridades a los datos que les permitan investigar los delitos de manera efectiva.

3.2 Acceso transfronterizo a pruebas electrónicas para investigaciones penales

Otra cuestión relevante relativa al acceso de las autoridades a las pruebas electrónicas es que en muchos casos los proveedores que las tienen en su poder se encuentran situados en una jurisdicción diferente a aquella en la que se produce la investigación.⁶⁷ Esto dificulta y retrasa sobremanera el acceso transfronterizo llevando a que haya muchas investigaciones que se abandonen sin ningún resultado. Por ello la UE ha creado un nuevo instrumento que son las órdenes europeas de entrega (EPOC) y conservación de pruebas electrónicas (EPOC-PR) a efectos de enjuiciamiento penal.⁶⁸

De hecho, una de las causas de su creación fue que, con motivo de los atentados terroristas perpetrados en Bruselas, los ministros de Justicia y Asuntos de Interior de los Estados miembros subrayaron la necesidad, con carácter prioritario, de proteger y obtener más rápida y eficazmente pruebas digitales, y de determinar medidas concretas para llevarlo a cabo.⁶⁹

El Reglamento se aplicará a los prestadores que ofrezcan servicios en la UE y aquellos establecidos fuera de la misma tendrán que nombrar un representante, como ocurre con el Reglamento sobre contenidos terroristas.

⁶⁷ Véase ANA GASCÓN MARCÉN, «El impulso para la regulación internacional del acceso transfronterizo a las pruebas electrónicas y los derechos humanos». *Cuadernos de Derecho Transnacional*, 15(1), 2023, pp. 385-402. Este artículo describe las diferentes soluciones utilizadas por China, Estados Unidos y la UE y algunos mecanismos internacionales para acceder a pruebas electrónicas para investigaciones penales y los problemas que plantean sus diferentes enfoques desde una perspectiva de derechos humanos.

⁶⁸ Reglamento (UE) 2023/1543 del Parlamento Europeo y del Consejo, de 12 de julio de 2023, sobre las órdenes europeas de producción y las órdenes europeas de conservación a efectos de prueba electrónica en procesos penales y de ejecución de penas privativas de libertad a raíz de procesos penales, DOUE L 191 de 28.7.2023, pp. 118-180. Véase ANA GASCÓN MARCÉN, «Las órdenes europeas de entrega y conservación de pruebas electrónicas: Evaluación de la propuesta de la Comisión Europea», *El mercado único en la Unión Europea: balance y perspectivas jurídico-políticas*, Dykinson, 2019, pp. 1121-1134.

⁶⁹ Declaración conjunta de los ministros de Justicia y Asuntos de Interior y los representantes de las instituciones de la Unión Europea, de 24 de marzo de 2016

Se disponen salvaguardas diferentes si se trata de datos de los abonados, datos solicitados con el único fin de identificar al usuario, datos de tráfico o datos de contenido, al considerarse la injerencia de diferente magnitud, cristalizándose así lo establecido por el TJUE en *La Quadrature du Net*. Por ejemplo, una EPOC para obtener datos de tráfico (excepto para obtener datos solicitados con el único fin de identificar al usuario) o de contenido, solamente podrá ser emitida para las infracciones penales punibles con una pena máxima privativa de libertad de al menos tres años. No obstante, se hace una excepción para ciertos delitos como el terrorismo.

Lo interesante de estas órdenes es que el Estado emisor podrá dirigir las directamente a los proveedores, convirtiéndose así en un nuevo caso de cooperación entre autoridades estatales y proveedores para luchar contra el terrorismo (y otros tipos de delito). No obstante, habrá que notificar a la autoridad del Estado de ejecución⁷⁰ cuando la EPOC sea para conseguir el tipo de datos más sensibles anteriormente citados y podrán denegarla si vulnera inmunidades o privilegios concedidos en virtud del Derecho del Estado de ejecución o los datos solicitados estén protegidos por la libertad de prensa o la libertad de expresión en otros medios de comunicación que impidan la ejecución de la orden; existan motivos fundados para suponer que la ejecución de la orden conllevaría una vulneración manifiesta de un derecho fundamental pertinente establecido en la CDFUE; o la ejecución de la orden sería contraria al principio *non bis in idem*. Como se pueden ver se han incorporado salvaguardas para los derechos fundamentales que se podrían ver menoscabados por el uso de las órdenes.

La colaboración directa con los proveedores busca sobre todo la rapidez, por lo que en general se cuenta con un plazo de 10 días para ejecutar una EPOC. Esto se agiliza en casos de urgencia puesto que el plazo se reduce a 8 horas. Esto puede ser especialmente útil en casos de terrorismo, dado que se define “caso urgente” como una situación en la que exista una amenaza inminente para la vida, la integridad física o la seguridad de una persona o para una infraestructura esencial, cuando la perturbación o destrucción de dicha infraestructura esencial pueda dar lugar a una amenaza inminente para la vida, la integridad física o la seguridad de una persona, también

⁷⁰ Estado miembro en el que tenga su sede el establecimiento designado o en el que resida el representante legal.

mediante perjuicios graves al suministro de productos básicos para la población o para el ejercicio de las funciones esenciales del Estado.

Böse se mostró muy crítico con estos instrumentos. Según él, la propuesta de la Comisión extendía la jurisdicción sobre los proveedores establecidos y los datos almacenados en Estados no miembros y, por lo tanto, comprometía el funcionamiento de la cooperación internacional con terceros Estados y generaba incertidumbre legal tanto para los proveedores como para los usuarios. En su opinión, el mecanismo de cooperación propuesto privaba a la persona de la protección que brinda el marco tradicional de cooperación internacional y lo más adecuado habría sido reforzar la orden europea de investigación como alternativa.⁷¹

López Amigo felicitó a la UE por esta iniciativa por crear instrumentos específicos, adaptados a las características especiales de las pruebas electrónicas, no obstante, subrayó varios de sus desaciertos, siendo el más problemático el que las órdenes no se dirijan a una autoridad judicial del Estado de ejecución, sino directamente a los proveedores, a los que se les impone la obligación de cumplirlas (con posibilidad de imposición de sanciones pecuniarias). A este autor le resultaba paradójico que la Comisión Europea caracterizara las órdenes como instrumentos de reconocimiento mutuo en el ámbito de la cooperación judicial penal, pero articulara un sistema, no de comunicación directa entre autoridades judiciales, sino entre una autoridad judicial y un proveedor, que es una entidad privada. Con ello, el control judicial en el Estado de ejecución será sólo eventual, en una materia que afecta de lleno a los datos personales y la privacidad y, por tanto, a los derechos fundamentales.⁷² González Fuster y Stefan han criticado también que la legalidad de la opción de otorgar automáticamente niveles más bajos de privacidad y protección a los datos de los abonados y a los de acceso es dudosa, ya que se basa en la suposición no verificada de que estas categorías de información son menos sensibles por defecto.⁷³

⁷¹ MARTIN BÖSE, *An assessment of the Commission's proposals on electronic evidence*, Parlamento Europeo, 2018.

⁷² LUIS GÓMEZ AMIGO, «Las órdenes europeas de entrega y conservación de pruebas penales electrónicas: una regulación que se aproxima», *Revista Española de Derecho Europeo*, núm. 71, 2019.

⁷³ MARCO STEFAN y GLORIA GONZÁLEZ, *Cross-border Access to Electronic Data through Judicial Cooperation in Criminal Matters. State of the art and latest developments in the EU and the US*, CEPS Papers No. 2018-07, 2018. También fue bastante crítico el Comité Europeo

Varias ONG (asociaciones de derechos digitales, medios de comunicación, periodistas, proveedores...) pidieron sin éxito al Parlamento Europeo que votará en contra del reglamento porque estaban preocupadas por el riesgo de que los mecanismos propuestos socavarán gravemente los derechos fundamentales, incluida la libertad de prensa, la privacidad, el derecho a un juicio justo y los deberes de secreto profesional y confidencialidad. En concreto consideraban que el sistema de notificación quedó muy reducido y sería básicamente ineficaz, porque en la práctica diaria de las autoridades policiales y judiciales, probablemente será la excepción y no la regla. Como resultado, el instrumento no cumplía su promesa de brindar seguridad jurídica a los proveedores y corría el riesgo de ser objeto de abusos para atacar a periodistas, defensores de los derechos humanos, activistas, opositores políticos y abogados. Además, el Reglamento no tenía en cuenta los contextos nacionales con un estado de derecho debilitado y mayores riesgos de represión política (como en Polonia o Hungría). Asimismo, en materia de secreto profesional y confidencialidad, el Reglamento prevé salvaguardias mal diseñadas que, en la práctica, no impedirán el acceso ilegítimo a las comunicaciones y datos de médicos, trabajadores sociales y abogados, incumpliendo sus obligaciones legales para con sus pacientes y clientes. En opinión de estas ONG, en la mayoría de los casos, los proveedores seguirán siendo la única defensa contra la extralimitación de las fuerzas del orden. Desafortunadamente, incluso su poder para detener la ejecución de órdenes es limitado y claramente desincentivado.⁷⁴

La UE además está negociando un acuerdo de acceso a pruebas electrónicas con Estados Unidos bajo el paraguas de la *CLOUD Act*.⁷⁵ El acuerdo busca

de Protección de Datos, *Opinion 23/2018 on Commission proposals on European Production and Preservation Orders for electronic evidence in criminal matters*.

⁷⁴ *Joint letter to the European Parliament Plenary vote on the “e-evidence package” Regulation and Directive on “European production and preservation orders for electronic evidence in criminal matters” and “legal representatives”*, 12 de junio de 2023. Disponible en: <https://edri.org/wp-content/uploads/2023/06/Joint-Letter-Plenary-Vote-E-evidence-13-June-2023.pdf> (última consulta: 18-09-23).

⁷⁵ Véase THEODORE CHRISTAKIS y FABIEN TERPAN, «EU–US negotiations on law enforcement access to data: divergences, challenges and EU law procedures and options», *International Data Privacy Law*, vol. 11, n° 2, 2021, pp. 81-106, <https://doi.org/10.1093/idpl/ipaa022> (última consulta: 08/09/2023).

evitar conflictos legales y establecer reglas comunes para las órdenes de una autoridad judicial en un Estado para obtener pruebas electrónicas en poder de un proveedor establecido en otro. También debería permitir la transferencia de pruebas electrónicas directamente, y de manera recíproca, por parte de un proveedor en un Estado a una autoridad solicitante en otro.

La UE también formó parte de la negociación del Segundo Protocolo adicional al Convenio sobre la Ciberdelincuencia, relativo a la cooperación reforzada y la revelación de pruebas electrónicas.⁷⁶ Este establece que las Partes adoptarán las medidas que sean necesarias para facultar a sus autoridades competentes para dictar un requerimiento que se dirija directamente a un proveedor que se encuentre en otra Parte, con el fin de obtener información específica almacenada relativa a los abonados, que obre en poder o esté bajo el control de dicho proveedor, cuando la información relativa a los abonados sea necesaria para las investigaciones o procesos penales específicos de la Parte emisora. Además, crea un sistema de asistencia mutua en situaciones de emergencia, lo que puede ser aplicable en casos de terrorismo dado que se entiende como tal la situación en la que exista un riesgo significativo e inminente para la vida o la seguridad de una o más personas físicas. De hecho, el Informe explicativo del Protocolo pone como ejemplo el escenario inmediatamente posterior a un ataque terrorista en el que las autoridades buscan averiguar con quién se comunicaron los atacantes para determinar si son inminentes nuevos ataques.

El problema es que los Estados parte del Convenio de Budapest y probablemente del Segundo Protocolo son muy heterogéneos y no todos presentan las mismas salvaguardas de derechos humanos.⁷⁷ Así en el Protocolo se ha intentado salvar esta cuestión fundamentalmente incluyendo un artículo

⁷⁶ Véase ANA GASCÓN MARCÉN, «La Unión Europea y los convenios internacionales elaborados en el marco del Consejo de Europa», *Interacciones entre el Derecho de la Unión Europea y el Derecho Internacional Público*, Tirant lo Blanch, 2023, pp. 227-242 y de la misma autora «The Budapest Convention and the new initiative for a United Nations Convention to fight cybercrime», *Global Cybersecurity and International Law*, Routledge (en prensa).

⁷⁷ Desgraciadamente no todas las partes de estos convenios lo son a su vez del Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal del Consejo de Europa conocido como Convenio 108, o de su versión modificada, conocida como Convenio 108+. Estados Unidos ni siquiera tiene una ley general de protección de datos personales.

en el que se resumen algunas de las principales garantías relacionadas con la protección de los datos personales en relación con: finalidad y utilización, calidad e integridad, datos delicados, períodos de conservación, decisiones automatizadas, seguridad de los datos e incidentes que afecten a la seguridad, transparencia y notificación, consulta y rectificación y vías de recurso judiciales y extrajudiciales. Sin embargo, es imposible resumir un régimen maduro de protección de datos en un simple artículo.

Carrera et al se han mostrado tremendamente críticos con la proliferación de iniciativas que promueven nuevas herramientas internacionales de cooperación público-privada directa para la recopilación de datos con fines de aplicación de la ley, porque esto plantea desafíos cruciales de coherencia y seguridad jurídica, desde la perspectiva de la protección de datos y la justicia penal de la UE.⁷⁸ En su opinión, normas como la *CLOUD Act*, o iniciativas de cooperación internacional como el Protocolo al Convenio de Budapest, pueden afectar las normas comunes de la UE o alterar su alcance. La supervisión judicial efectiva de las solicitudes de datos es especialmente importante para evitar que comprometan la esencia del acervo de derechos fundamentales de la UE. Respecto a las negociaciones sobre el Protocolo, defendieron que la participación de la UE debía tener como objetivo estrictamente garantizar que se preservara la integridad del acervo comunitario existente. En su opinión, las EPOC no deberían tomarse como punto de referencia para el desarrollo de acciones o posiciones exteriores de la UE y debía evitarse la adopción de instrumentos que permitirían a las autoridades de terceros países acceder a datos sujetos a la jurisdicción de la UE, fuera de los instrumentos de cooperación judicial de la UE existentes. En conclusión, argumentaban que el objetivo de dotar a las autoridades encargadas de hacer cumplir la ley de nuevas herramientas para luchar contra la ciberdelincuencia y el terrorismo no debe justificar la introducción de instrumentos incompatibles con la legislación de la UE.

Tropina respecto a las EPOC, la *CLOUD Act* y el Protocolo también considera que reemplazar los mecanismos tradicionales de asistencia legal mutua con solicitudes directas a los proveedores puede conducir a la

⁷⁸ SERGIO CARRERA ET AL., *Cross-border data access in criminal proceedings and the future of digital justice: Navigating the current legal framework and exploring ways forward within the EU and across the Atlantic*. CEPS Task Force Report, 2020, pp. 77-78.

privatización de la aplicación de la ley y, en última instancia, tener un efecto severo en la protección de los derechos fundamentales en la UE y más allá.⁷⁹

4. Conclusiones

Los Estados miembros de la UE han tomado en los últimos años múltiples medidas para luchar contra el terrorismo, y uno de los ámbitos en los que se han centrado sus nuevas iniciativas es el digital, ya sea para impedir compartir contenidos terroristas o para seguir las huellas de aquellos que han perpetrado o estaban preparando un ataque terrorista. Para poder poner en marcha estas medidas hace falta la cooperación de los proveedores de servicios de Internet que se han convertido en actores muy relevantes en la lucha antiterrorista.

Es muy positivo que la UE esté buscando crear nuevas herramientas para luchar contra el terrorismo en el ámbito digital porque sin duda los terroristas están haciendo uso de muchas de las oportunidades que les brinda el ciberespacio. Los proveedores de servicios de Internet deben estar sometidos a obligaciones de diligencia debida, pero éstas no deben ir demasiado lejos llevándoles al sobrebloqueo de contenidos para evitar sanciones o ponerles en la posición de ser ellos los únicos que puedan defender los derechos humanos de sus usuarios porque ése no es su papel. Además, no todos los proveedores son iguales no tienen los mismos recursos ni el mismo nivel de riesgo y eso debe también tenerse en cuenta. Además, es necesario ser consciente de que algunas de estas medidas tienen efecto extraterritorial y pueden ser copiadas por otros Estados terceros con un régimen general mucho menos garantista.

El objetivo de los nuevos instrumentos ya sean las órdenes de retirada de contenidos, conservación de datos o producción y conservación de pruebas electrónicas es mejorar y proteger la seguridad pública, lo que es uno de los objetivos legítimos para limitar derechos fundamentales. En particular, estas herramientas han sido fuertemente criticadas por su impacto en derechos como la privacidad, protección de datos personales o acceso a un recurso

⁷⁹ TATIANA TROPINA, «The EU and Access to Electronic Evidence: Privatisation of Law Enforcement?», *Cybersecurity Policy in the EU and South Korea from Consultation to Action. New Security Challenges*. Palgrave Macmillan, 2022, pp. 215-232.

judicial efectivo por eso es importante asegurarnos de evaluar su impacto y así saber si son necesarias y proporcionales en una sociedad democrática.

En general, desde las propuestas de la Comisión de órdenes de retirada o bloqueo de contenidos terroristas o EPOC y EPOC-PR al contenido final de ambos reglamentos se incluyeron varias nuevas salvaguardas de derechos a instancias del Parlamento Europeo que deben ser bienvenidas, si bien en algunos aspectos persisten las lagunas y las dudas de la compatibilidad de algunos de sus elementos con la Carta de los Derechos Fundamentales de la UE y la jurisprudencia del Tribunal Europeo de Derechos Humanos.

Se ha visto que en el pasado el TJUE ha anulado normas como lo hizo en *Digital Rights Ireland* con la Directiva de conservación de datos por no respetar los derechos fundamentales a los que deben someterse todas las normas de la UE. Si bien también hemos podido observar que el TJUE está dispuesto a hacer mayores concesiones cuando las medidas buscan proteger la seguridad nacional (*La Quadrature du Net*), como podría ocurrir con las medidas antiterroristas. El TJUE en este ámbito parece haber modificado su jurisprudencia y llegado a un compromiso por tratarse de este objetivo especialmente relevante para los Estados, que por otra parte en muchos casos no habían modificado sus legislaciones incluso con el conocimiento de estar incumpliendo el derecho de la UE.

También se ha observado que el TJUE ha optado por exigir diferentes niveles de protección según la naturaleza de los datos, ya que considera que la magnitud de la injerencia puede variar, lo que ha sido seguido por la regulación de las EPOC, EPOC-PR y el Segundo Protocolo del Convenio de Budapest.

Además, se tiende a incluir medidas de naturaleza urgente, la retirada de contenidos tiene que realizarse en una hora, y las EPOC y EPOC-PR y el Segundo Protocolo tienen modalidades específicas para casos de urgencia que supongan una considerable reducción de plazos. Esto está pensado para casos en los que esté en riesgo la seguridad y vida de las personas siendo el ejemplo arquetípico el del terrorismo. Incluso en normas como la DSA se han incluido mecanismos de crisis para casos como éste.

En relación con la DSA, sin ser una norma que esté destinada a luchar contra el terrorismo sin duda varios de sus preceptos tendrán impacto en la misma, dada la obligación de las grandes plataformas de evaluar los riesgos sistémicos a los que pueden contribuir y tener que tomar medidas para mitigarlos.

Bibliografía

- BARATA, J., *New EU Proposal on the Prevention of Terrorist Content Online*, Center for Internet and Society, 2018
- BÖSE, M., *An assessment of the Commission's proposals on electronic evidence*, Parlamento Europeo, 2018
- BROWN, I. y KORFF, D., «Terrorism and the proportionality of internet surveillance.», *European Journal of Criminology*, vol. 6, nº 2, 2009, pp. 119-134
- BSR, *Human Rights Assessment. Global Internet Forum to Counter Terrorism*. 2021, disponible en <https://www.bsr.org/reports/BSR-GIFCT-Report.pdf> (última consulta: 18-09-23)
- CARRERA S. *et al.*, *Cross-border data access in criminal proceedings and the future of digital justice: Navigating the current legal framework and exploring ways forward within the EU and across the Atlantic*. CEPS Task Force Report, 2020, pp. 77-78
- CASTELLÓ PASTOR, J. J., «Exoneración de responsabilidad de los prestadores de servicios de la información en la sección 230 de la Communications Decency Act estadounidense», *Revista Aranzadi de derecho y nuevas tecnologías*, nº 39, 2015, pp. 175-194
- CASTELLÓ PASTOR, J. J., «Nuevo régimen de responsabilidad de los servicios digitales que actúan como intermediarios a la luz de la propuesta de Reglamento relativo a un mercado único de servicios digitales», *Desafíos jurídicos ante la integración digital: aspectos europeos e internacionales*, Aranzadi, 2021, pp. 37-76
- CHRISTAKIS, T. y TERPAN, F., «EU–US negotiations on law enforcement access to data: divergences, challenges and EU law procedures and options», *International Data Privacy Law*, vol. 11, nº 2, 2021, pp. 81-106, <https://doi.org/10.1093/idpl/ipaa022> (última consulta: 08/09/2023)
- CITRON, D. K., *Extremist Speech, Compelled Conformity, and Censorship Creep*, University of Maryland Francis King Carey School of Law Legal Studies Research Paper No. 2017-12
- CITRON, D. K., *What to Do about the Emerging Threat of Censorship Creep on the Internet*, Cato Institute, 28-11-2017, disponible en <https://www.cato.org/policy-analysis/what-do-about-emerging-threat-censorship-creep-internet> (última consulta: 18-09-23)

- COMITÉ EUROPEO DE PROTECCIÓN DE DATOS, *Opinion 23/2018 on Commission proposals on European Production and Preservation Orders for electronic evidence in criminal matters*
- CONWAY, M. *et al.* (eds.), *Terrorist use of the Internet*, OTAN, 2017
- CRUZ ÁNGELES, J., «Las obligaciones jurídico-comunitarias de las grandes plataformas proveedoras de servicios digitales en la era del metaverso», *Cuadernos de Derecho Transnacional*, 14(2), 2022, pp. 294-318, disponible en <https://doi.org/10.20318/cdt.2022.7186> (última consulta: 18-09-23)
- DE GREGORIO, G., «Fighting Terrorism Online: Censorship, Platforms and Freedom of Expression across the Atlantic», *Virtual freedoms, Terrorism and the Law*, Routledge, 2021, pp. 95-117
- DE GREGORIO, G., «The rise of digital constitutionalism in the European Union», *International Journal of Constitutional Law*, vol. 19, t. 1, 2021, pp. 41-70, disponible en <https://doi.org/10.1093/icon/moab001> (última consulta: 18-09-23)
- DOUEK, E., *The Rise of Content Cartels*, Knight First Amendment Institute, 2020, disponible en <https://knightcolumbia.org/content/the-rise-of-content-cartels> (última consulta: 18-09-23)
- DUARTE, N., LLANSO, E. y LOUP, A., *Mixed Messages? The Limits of Automated Social Media*, Center for Democracy & Technology, 2017
- DUTKIEWICZ, L. y KRACK., N., «All eyes riveted on the trilogue closed doors of the Proposal for a Regulation on preventing the dissemination of terrorist content online [Part I]», *KU Leuven CiTIP Blog*, 24-11-2020, disponible en <https://www.law.kuleuven.be/citip/blog/all-eyes-riveted-on-the-trilogue-closed-doors-of-the-proposal-for-a-regulation-on-preventing-the-dissemination-of-terrorist-content-online-part-i/> (última consulta: 18-09-23)
- DUTKIEWICZ, L. y KRACK., N., «How to notice without looking: the ‘algorithmization’ of terrorist content moderation in the Proposal for a Regulation on preventing the dissemination of terrorist content online [Part II]», *KU Leuven CiTIP Blog*, 25-11-2020, disponible en <https://www.law.kuleuven.be/citip/blog/how-to-notice-without-looking-the-algorithmization-of-terrorist-content-moderation-in-the-proposal-for-a-regulation-on-preventing-the-dissemination-of-terrorist-content-online-part-ii/> (última consulta: 18-09-23)
- EDRI ET AL., *How-to: Fundamental rights-compliant removal orders in the Terrorist Content Online Regulation*, 28-10-2020, disponible en

- https://edri.org/wp-content/uploads/2020/11/CivilSocietyBriefing_TCO RemovalOrders_Oct2020.pdf (última consulta: 18-09-23)
- EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS, Opinion 2/2019 on the Proposal for a Regulation on preventing the dissemination of terrorist content online and its fundamental rights implications, 12-2-2019, disponible en https://fra.europa.eu/sites/default/files/fra_uploads/fra-2019-opinion-online-terrorism-regulation-02-2019_en.pdf (última consulta: 18-09-23)
- EUROPOL, *EU IRU Transparency Report 2021*, 2022. Disponible en https://www.europol.europa.eu/cms/sites/default/files/documents/EU_IRU_Transparency_Report_2021.pdf (última consulta: 18-09-23)
- EUROPOL, *Online Jihadist Propaganda 2021 in review*, Publications Office of the European Union, Luxemburgo, 2022
- FINCK, M., *Artificial intelligence and online hate speech*, Centre on Regulation in Europe, 2019
- GASCÓN MARCÉN, A., «El impulso para la regulación internacional del acceso transfronterizo a las pruebas electrónicas y los derechos humanos», *Cuadernos de Derecho Transnacional*, 15(1), 2023, pp. 385-402
- GASCÓN MARCÉN, A., «El nuevo Reglamento europeo para la prevención de contenidos terroristas en línea», *Retos del Estado de Derecho en materia de inmigración y terrorismo*, Iustel, 2022, pp. 525-546
- GASCÓN MARCÉN, A., «El Reglamento General de Protección de Datos como modelo de las recientes propuestas de legislación digital europea», *Cuadernos de Derecho Transnacional*, vol. 13, t. 2, 2021
- GASCÓN MARCÉN, A., «La responsabilidad de los intermediarios de Internet en la Unión Europea: iniciativas recientes y perspectivas de futuro», *Desafíos jurídicos ante la integración digital: aspectos europeos e internacionales*, Aranzadi, 2021, pp. 133-160
- GASCÓN MARCÉN, A., «La sentencia La Quadrature du Net y el futuro de la normativa de conservación de datos», *Estudios sobre Jurisprudencia Europea: materiales del VI Encuentro anual del Centro español del European Law Institute*, Sepin, 2023, pp. 656-673
- GASCÓN MARCÉN, A., «La Unión Europea y los convenios internacionales elaborados en el marco del Consejo de Europa», *Interacciones entre el Derecho de la Unión Europea y el Derecho Internacional Público*, Tirant lo Blanch, 2023, pp. 227-242

- GASCÓN MARCÉN, A., «Las órdenes europeas de entrega y conservación de pruebas electrónicas: Evaluación de la propuesta de la Comisión Europea», *El mercado único en la Unión Europea: balance y perspectivas jurídico-políticas*, Dykinson, 2019, pp. 1121-1134
- GASCÓN MARCÉN, A., «The Budapest Convention and the new initiative for a United Nations Convention to fight cybercrime», *Global Cybersecurity and International Law*, Routledge, 2024
- GÓMEZ AMIGO, I., «Las órdenes europeas de entrega y conservación de pruebas penales electrónicas: una regulación que se aproxima», *Revista Española de Derecho Europeo*, núm. 71, 2019
- GONZÁLEZ PASCUAL, M. I., «EL TJUE como garante de los derechos en la UE a la luz de la sentencia Digital Rights Ireland», *Revista de Derecho Comunitario Europeo*, Año nº 18, nº 49, 2014, pp. 943-971
- GRANGER, M.-P. y IRION, K., «The Court of Justice and the Data Retention Directive in Digital Rights Ireland: Telling Off the EU Legislator and Teaching a Lesson in Privacy and Data Protection», *European Law Review*, nº 6, 2014, pp. 835-850
- HADI KHATIB, A. y KAYYALI, D., «YouTube Is Erasing History. Under pressure to remove «extremist content», platforms are purging vital human rights evidence», *The New York Times*, 23-10-2019, disponible en <https://www.nytimes.com/2019/10/23/opinion/syria-youtube-content-moderation.html> (última consulta: 18-09-23)
- HELLER, B., *Combating Terrorist-Related Content through AI and Information Sharing*, Transatlantic Working Group, 2019, disponible en https://www.ivir.nl/publicaties/download/Hash_sharing_Heller_April_2019.pdf (última consulta: 18-09-23)
- HUMAN RIGHTS WATCH, «*Video Unavailable*»: *Social Media Platforms Remove Evidence of War Crimes*, Human Rights Watch. 2020, disponible en <https://www.hrw.org/report/2020/09/10/video-unavailable/social-mediaplatforms-remove-evidence-war-crimes> (última consulta: 18-09-23)
- KAYYALI, D., «European «terrorist content» proposal is dangerous for human rights globally», *Witness*, 6-12-2018, disponible en <https://blog.witness.org/2018/12/european-terrorist-content-proposal-dangerous-human-rights-globally/> (última consulta: 18-09-23)
- KELLER, D., «Empirical evidence of over-removal by internet companies under intermediary liability laws: an updated list», Center for Internet

- and Society, 8-2-2-2021, disponible en <http://cyberlaw.stanford.edu/blog/2021/02/empirical-evidence-over-removal-internet-companies-under-intermediary-liability-laws> (última consulta: 18-09-23)
- KUCZERAWY, A., *The proposed Regulation on preventing the dissemination of terrorist content online: safeguards and risks for freedom of expression*, Center for Democracy and Technology, 2018
- LLANSÓ, E., «Platforms Want Centralized Censorship. That Should Scare You», *Wired*, 18-4-2019, disponible en <https://www.wired.com/story/platforms-centralized-censorship/> (última consulta: 18-09-23)
- MACKLIN, G., «The Christchurch attacks: Livestream terror in the viral video age», *CTC Sentinel*, vol. 12, t. 6, 2019, pp. 18-29
- MURRAY, D. y FUSSEY, P., «Bulk Surveillance in the Digital Age: Rethinking the Human Rights Law Approach to Bulk Monitoring of Communications Data», *Israel Law Review*, vol. 52, nº 1, 2019, pp. 31-60
- O'FLAHERTY, K., «YouTube keeps deleting evidence of Syrian chemical weapon attacks», *Wired*, 26-06-2018, disponible en <https://www.wired.co.uk/article/chemical-weapons-in-syria-youtube-algorithm-delete-video> (última consulta: 18-09-23)
- POLO ROCA, A., «La regulación sobre la conservación de datos en el sector de las comunicaciones electrónicas o telecomunicaciones: estado de la cuestión», *IDP: Revista d'Internet, dret i política* 33, 2021
- SAJFERT, J., «Bulk data interception/retention judgments of the CJEU – A victory and a defeat for privacy», *European Law Blog*. 26/10/2020. <https://europeanlawblog.eu/2020/10/26/bulk-data-interception-retention-judgments-of-the-cjeu-a-victory-and-a-defeat-for-privacy/> (última consulta: 18-09-23)
- SANDER, B., «Democratic Disruption in the Age of Social Media: Between Marketized and Structural Conceptions of Human Rights Law». *European Journal of International Law*. 32 (1), 2021 <https://doi.org/10.1093/ejil/chab022> (última consulta: 18-09-23)
- SCHEININ, MARTIN «The EU Regulation on Terrorist Content: An Emperor without Clothes», *Verfassungsblog*, 30-1-2019, disponible en <https://verfassungsblog.de/the-eu-regulation-on-terrorist-content-an-emperor-without-clothes/> (última consulta: 18-09-23)
- SHAHBAZ, A. y FUNK, A., *Freedom on the Net 2019: The Crisis of Social Media*, Freedom House, 2019 <https://freedomhouse.org/sites/>

- default/files/2019-11/11042019_Report_FH_FOTN_2019_final_Public_Download.pdf (última consulta: 18-09-23)
- SHENKMAN, C., THAKUR, D. y LLANSÓ, E., *¿Do You See What I See? Capabilities and Limits of Automated Multimedia Content Analysis*, Center for Democracy & Technology, 2021, disponible en <https://cdt.org/insights/do-you-see-what-i-see-capabilities-and-limits-of-automated-multimedia-content-analysis/> (última consulta: 18-09-23)
- STEFAN, M. y GONZÁLEZ, G., *Cross-border Access to Electronic Data through Judicial Cooperation in Criminal Matters. State of the art and latest developments in the EU and the US*, CEPS Papers No. 2018-07, 2018
- TECH AGAINST TERRORISM, *Government Transparency Reporting on Online Counterterrorism Efforts*, disponible en <https://static1.square-space.com/static/609d273957ee294d03d8dadf/t/60fe84736b5d5b2618fdb95/1627292788720/TAT+Guidelines+-+Government+transparency+reporting+on+online+counterterrorism+efforts.pdf> (última consulta: 18-09-23)
- TECH AGAINST TERRORISM, *The Online Regulation Series. The Handbook*, 2021, disponible en <https://www.techagainstterrorism.org/wp-content/uploads/2021/07/Tech-Against-Terrorism-%E2%80%93-The-Online-Regulation-Series-%E2%80%93-The-Handbook-2021.pdf> (última consulta: 18-09-23)
- TECH AGAINST TERRORISM, *Trends in Terrorist and Violent Extremist Use of the Internet. Q1-Q2 2021*, 2021, disponible en <https://www.techagainstterrorism.org/wp-content/uploads/2021/07/Tech-Against-Terrorism-Q1-Q2-TVEC-Trends-2021.pdf> (última consulta: 18-09-23)
- TERUEL LOZANO, G. M. «Una lectura garantista de las nuevas tendencias en la lucha europea contra la difusión de mensajes terroristas en Internet», *Revista de Derecho Constitucional Europeo*, vol. 34. Julio-Diciembre de 2020
- TODOROVIC, B. y TRIFUNOVIC, D., «Chapter 19. Prevention of (Ab-)Use of the Internet for Terrorist Plotting and Related Purposes», *Handbook of Terrorism Prevention and Preparedness*, ICCT Press, La Haya, 2020, pp. 616-643
- TRACOL, X., «The two judgments of the European Court of Justice in the four cases of Privacy International, La Quadrature du Net and Others,

French Data Network and Others and Ordre des Barreaux francophones et germanophone and Others: The Grand Chamber is trying hard to square the circle of data retention», *Computer Law & Security Review*, vol. 41. 2021

TROPINA, T., «The EU and Access to Electronic Evidence: Privatisation of Law Enforcement? », *Cybersecurity Policy in the EU and South Korea from Consultation to Action. New Security Challenges*. Palgrave Macmillan, 2022, pp. 215-232.

VAN HOBOKEN, J., The Proposed EU Terrorism Content Regulation: Analysis and Recommendations with Respect to Freedom of Expression Implications, Transatlantic Working Group, 2019, p. 7, disponible en https://www.ivir.nl/publicaties/download/TERREG_FoE-ANALYSIS.pdf (última consulta: 18-09-23)

La financiación del terrorismo: estructura, medios legales e ilegales y mecanismos de control

Terrorist financing: structure, legal and illegal means and control mechanisms

Carmen Parra Rodríguez
Francisco Villacampa Mejía

Resumen: La financiación del terrorismo es un fenómeno complejo que implica la obtención de recursos económicos para llevar a cabo actividades que provocan el terror en la sociedad utilizando acciones violentas. La estructura financiera de estas organizaciones puede involucrar una combinación de fuentes, como donaciones, extorsiones, tráfico de drogas, contrabando, u otras actividades ilícitas, existiendo también medios legales utilizados que a menudo incluyen el abuso de instituciones financieras, el uso de organizaciones caritativas y la manipulación de sistemas legales para encubrir las transacciones. Para combatir esta amenaza, los mecanismos de control se centran en la supervisión y regulación de las transacciones financieras, la colaboración internacional para intercambiar información de inteligencia, el congelamiento de activos sospechosos y la implementación de sanciones económicas. La coordinación entre gobiernos, instituciones financieras y organismos internacionales es esencial para prevenir

Abstract: Terrorist financing is a complex phenomenon that involves obtaining economic resources to carry out activities that provoke terror in society using violent actions. The financial structure of these organizations may involve a combination of sources, such as donations, extortion, drug trafficking, smuggling, or other illicit activities, and there are also legal means used that often include the abuse of financial institutions, the use of charitable organizations, and the manipulation of legal systems to cover up transactions. To combat this threat, control mechanisms focus on the supervision and regulation of financial transactions, international collaboration to exchange intelligence information, the freezing of suspicious assets, and the implementation of economic sanctions. Coordination between governments, financial institutions, and international organizations is essential to prevent and dismantle terrorist financing networks, ensuring the integrity of the global financial system.

y dismantelar las redes de financiamiento del terrorismo, asegurando la integridad del sistema financiero global.

Palabras clave: cooperación institucional; financiación; terrorismo; violencia; yihadismo.

Keywords: financing; institutional cooperation; jihadism; terrorism; violence.

Sumario: 1. Estructura de los grupos terroristas; 2. Principais formas de financiación de terrorismo; 2.1. Clasificación por grupos de las principales formas de financiación de las organizaciones terroristas; 2.2. Criterios para clasificar las formas de financiación de las organizaciones terroristas; 3. El origen de las fuentes de financiación: entre la legalidad y la ilegalidad; 3.1. Las fuentes de financiación de origen ilegal de los grupos terroristas; 3.2. Las fuentes de financiación de origen legal de los grupos terroristas; 3.2.1. Uso de Internet para difundir propaganda y recaudar fondos; 3.2.2. Microfinanciación; 3.2.3. Monedas virtuales; 3.2.4. Tarjetas de prepago; 3.2.5. Fideicomisos (del tipo *trust*); 4. El papel de las instituciones internacionales en la lucha contra la financiación del terrorismo; 4.1. El papel Naciones Unidas en el control de la financiación de los grupos terroristas; 4.1.1. Creación de un marco legal internacional; 4.1.2. Lista de sanciones; 4.1.3. Colaboración con organismos especializados en la lucha contra la financiación de terrorismo; 4.2. La función de la Unión Europea en la financiación de los grupos terroristas; 4.3. El papel de Interpol y Europol para combatir la financiación de los grupos terroristas; 5. Conclusiones.

1. Estructura de los grupos terroristas

Abordar la estructura que tienen los grupos terroristas en la actualidad, es un tema complejo y diverso. Este tipo de organizaciones criminales varían en tamaño, alcance, ideología y objetivos específicos. Es importante destacar la dificultad que tienen las agencias de seguridad e inteligencia para infiltrarse en este tipo de organizaciones con el objetivo de obtener información sobre ellas. Este escollo, es todavía mayor en el caso de las organizaciones terroristas de carácter yihadista. En la actualidad, la principal amenaza terrorista que se cierne sobre la humanidad, está representada por los grupos yihadistas. Este criminal fenómeno actúa en cualquier parte del mundo, pero tiene

como principales lugares de acción, el Norte de África, Oriente medio, el Sahel, Cuerno de África, Irak, Afganistán y Pakistán.¹ Es fundamental tener en cuenta que la situación puede cambiar y que pueden surgir nuevos grupos o producirse modificaciones en la actividad de los existentes. Además, las perspectivas sobre qué grupos son considerados “terroristas” pueden variar según la región y la opinión política.

Si bien la estructura de un grupo terrorista puede variar considerablemente según su ideología, objetivos y contexto, muchas de ellos comparten una serie de elementos que se repiten independientemente de su área de actuación. La estructura típica que se puede encontrar en muchos grupos terroristas es la siguiente:

a) Liderazgo centralizado o descentralizado

Centralizado: Algunos grupos terroristas tienen una estructura jerárquica con un líder supremo y varias capas de mando. El líder toma decisiones estratégicas y establece objetivos para el grupo. En las organizaciones yihadistas la estructura centralizada la ocupa el Emir que actúa como líder supremo con autoridad sobre el grupo tomando las decisiones clave para el grupo. Es el caso de organizaciones como Al Qaeda o Daesh, sus líderes, Bin Laden y Abu Bakr al-Bagdadi, ejercían un control cuasi absoluto sobre las acciones que se llevaban a cabo.

Descentralizado: Se refiere a que grupos pueden operar de manera descentralizada, con células independientes que actúan de manera autónoma

¹ A modo de ejemplo se muestran a continuación algunas de las más conocidas *ISIS* (Estado Islámico), organización que aunque ha perdido territorio en los últimos años, sigue siendo una amenaza en algunas regiones, especialmente en Oriente Medio. *Al-Qaeda* tiene su ámbito de actuación a nivel global, siendo tristemente conocido por los atentados perpetrados en Estados Unidos el 11 de septiembre de 2001. *Talibán* con presencia en Afganistán, involucrado en actividades terroristas que ha ido ganando notoriedad a lo largo de los años. *Boko Haram* grupo activo principalmente en Nigeria y algunas regiones de África Occidental. *Hezbollah* es una organización chiíta con base en el Líbano. *FARC* (Fuerzas Armadas Revolucionarias de Colombia) que aunque oficialmente han dejado de existir como grupo armado, algunos disidentes continúan participando en actividades ilegales. *Al-Shabaab* que está activo en Somalia y en algunas partes de África Oriental, *Al-Shabaab* tiene vínculos con *Al-Qaeda* junto a la que ha perpetrado numerosos ataques terroristas.

y pueden recibir apoyo estratégico pero con mayor independencia en la toma de decisiones. En la estructura descentralizada yihadista, ocupa este lugar la denominada «Shura Majlis» que es un Consejo consultivo compuesto por líderes religiosos y militares que asesoran al Emir en la toma de decisiones. En el caso de Al Qaeda, la «Shura» estaba formada por personas de máxima confianza de Bin Laden y con una dilatada experiencia en acciones desestabilizadoras. Del mencionado Consejo dependían cuatro comités: militar, financiero, asuntos religiosos y de información².

b) Células operativas

Muchos grupos terroristas dividen sus miembros en células operativas más pequeñas. Esto ayuda a minimizar la posibilidad de infiltración y facilita la realización de operaciones sin que todos los miembros conozcan el alcance completo de las actividades, lo que hace más compleja su identificación y control por parte de las fuerzas de seguridad.

c) Financiación

Los grupos terroristas requieren recursos financieros para llevar a cabo sus actividades. La captación de recursos proviene de diversas fuentes, tanto legales como ilegales. Destacando las siguientes: donaciones, actividades criminales (como el narcotráfico, el contrabando, tráfico de armas, trata de seres humanos, extorsión, secuestros), o incluso apoyo estatal en algunos casos (Irán y *Hezbollah*)

d) Reclutamiento y entrenamiento

Los grupos terroristas reclutan nuevos miembros para fortalecer sus filas. El entrenamiento puede incluir aspectos ideológicos, tácticos y técnicos necesarios para llevar a cabo sus operaciones.

² GUNARATNA, R., *Al Qaeda. Viaje al interior del terrorismo islamista*, Barcelona, Servidoc, 2003, p. 118-120.

e) Propaganda

Muchos grupos terroristas emplean la propaganda como una herramienta importante para difundir su mensaje y reclutar seguidores. Esto puede incluir comunicados, videos, sitios web y otros medios para difundir su ideología.

f) Redes Transnacionales

Las afiliaciones internacionales así como las alianzas con organizaciones similares en diferentes regiones del mundo fortalece la misión de estos grupos creando la sensación de tener redes muy amplias con alcance global. Asimismo estos grupos pueden tener conexiones con el crimen organizado para realizar actividades de contrabando y tráfico de drogas que les proporcionan recursos adicionales.

g) Infraestructura

Es muy útil el uso de bases de operaciones en áreas remotas o controladas por estos grupos terroristas para planificar y llevar a cabo actividades. Tenemos el caso de las zonas tribales entre Afganistán y Pakistán que han servido de base y refugio para los líderes y miembros de Al Qaeda. El uso de redes de comunicación encriptadas les permite además coordinar sus operaciones y evitar la detección de sus dispositivos de localización.

h) Objetivos ideológicos y motivaciones

Cada grupo terrorista tiene sus propios objetivos y motivaciones, que pueden estar relacionados con aspectos políticos, religiosos, étnicos o sociales, siendo la violencia y el terrorismo a menudo utilizados como medios para alcanzar estos objetivos. Es el caso por ejemplo del establecimiento de un Estado Islámico (*ISIS*) que fundamenta sus tentados en la interpretación de la ley islámica (*sharia*) o en la lucha contra los «enemigos del islam», ya sean gobiernos seculares, fuerzas extranjeras o grupos rivales.

Una vez establecida la estructura de los grupos terroristas es necesario conocer como se financian para llevar a cabo sus actuaciones.

2. Principales formas de financiación de terrorismo

Es importante destacar que cualquier forma de financiación del terrorismo es ilegal y condenable si bien las organizaciones terroristas utilizan diversas tácticas para obtener fondos siendo estas actividades perseguidas enérgicamente por la comunidad internacional. En este sentido, las Naciones Unidas, Interpol y Europol han venido informando acerca de la convergencia cada vez mayor entre la delincuencia organizada y el terrorismo, advirtiendo de la necesidad de implementar medidas y regulaciones a nivel nacional e internacional para rastrear y bloquear el flujo de fondos hacia estas organizaciones. Además, la cooperación entre países, la inteligencia financiera y las sanciones son herramientas clave para abordar esta amenaza global.

2.1. Clasificación por grupos de las principales formas de financiación de las organizaciones terroristas

Haciendo una aproximación a los principales sistemas de financiación de organizaciones terroristas se pueden clasificar de modo general en cuatro grupos³:

a) El patrocinio estatal

Fue un instrumento utilizado en el período de la Guerra Fría siendo los Estados los que armaron y financiaron a grupos terroristas a través de sus agencias de seguridad. No obstante este sistema cayó en los años noventa, fecha a partir de la cual el sistema de captación de recursos financieros tuvo un origen privado⁴, si bien en la actualidad existen algunas organizaciones islamistas (*Hezbollah*, en Líbano, *Hamás* y *Yihad* Islámica, en Palestina) que reciben financiación regular de los Gobiernos de Irán y Siria⁵.

³ JODI VITTORI, *Terrorist Financing and Resourcing*. New York, Palgrave Macmillan, 2011; y MIKEL BUESA BLANCO, «Financiación del terrorismo. Economía del terrorismo», *ICE*, nov-dic. n° 893, 2016, pp. 27-50.

⁴ MIKEL BUESA BLANCO, «War and Terrorism: The Predatory War Model» en MIKEL BUESA y THOMAS AUMERT, (eds.), *The Economic Repercussions of Terrorism*. Oxford: Oxford University Press, 2010.

b) Ejercicio de actividades ilegales por parte de las organizaciones terroristas

En este apartado se incluyen múltiples acciones dependiendo de la idiosincrasia y base territorial de las organizaciones. Las actividades más asiduas son el robo, las amenazas y el secuestro extorsivo, el contrabando, los tráficos ilegales de obras de arte, tabaco y drogas, la falsificación de tarjetas de crédito, la imposición forzada de servicios de protección, la venta de documentos de identidad falsificados, la explotación de redes de inmigración irregular y el tráfico ilícito de recursos naturales entre otros⁶.

c) Actividades legales o de apariencia legal

Estas acciones se caracterizan por la creación de empresas destinadas a obtener beneficios que servirán para sostener a organizaciones terroristas. Es el caso por ejemplo de empresas vinculadas a la *yihad* terrorista como es el caso de *Yihad Al Binaa*, una de las mayores firmas de construcción del Líbano vinculada a *Hezbollah*⁷. Sin embargo, en muchas ocasiones suelen ser negocios pequeños que permiten financiar células de ámbito local o que sirven para blanquear dinero obtenido por medios delictivos. Uno de los medios legales más utilizados es la *Hawala*, una red informal de envío de dinero que mueve millones de dólares al año fuera del alcance de Gobiernos y organismos internacionales.

d) Apoyo popular a través de cuotas de afiliación a entidades vinculadas con las organizaciones terroristas y donaciones directas o indirectas a través de instituciones de caridad

La aportación de donativos por parte de sociedades de beneficencia y organizaciones caritativas a las bandas armadas es habitual en el mundo islámico, siendo considerada una de las principales fuentes de financiación de la *yihad* terrorista. En este sentido el argumento utilizado ha sido el de

⁵ MARTIN RUDNER, «Hizbullah Terrorism Finance: Fund-Raising and Money-Laundering», *Studies in Conflict and Terrorism*, vol. 33, n° 8, 2010, pp. 700-715, esp. p. 702.

⁶ BUESA BLANCO, «Financiación del terrorismo...», *cit.*, p. 31

⁷ *Ibidem*, p.705.

desviar la *zakat* o limosna, por ser uno de los pilares del Islam, a la financiación de grupos terroristas. No obstante, son muy pocas las organizaciones que han podido ser acusadas de vincular su aportación con el terrorismo⁸, aunque por el contrario, si que se han podido probar las contribuciones directas de miembros de la comunidad musulmana a los grupos terroristas. Por ejemplo, las aportaciones de expatriados libaneses a Hezbolá⁹.

2.2. Criterios para clasificar las formas de financiación de las organizaciones terroristas

Las formas de financiación pueden ser abordadas desde diferentes perspectivas en función de las finalidades establecidas como objetivos por las organizaciones terroristas. Uno de los autores que han utilizado este sistema ha sido Freeman¹⁰, autor que ha establecido seis criterios para determinar las formas de financiación así como la forma en la que se obtienen los recursos por estos grupos tomando como pauta una serie de elementos que se enumeran a continuación:

a) La cuantía de los recursos necesarios para llevar a cabo la acción terrorista

Esta cuantía se determina en función de cuales sean sus fines políticos, su capacidad de movilización para reclutar militantes, sus necesidades de infraestructura y armamento, y el desarrollo de sus actividades ideológicas, de propaganda y de atención social dirigidas a su población de referencia. Estos recursos son limitados por cuanto su fin último no es obtener rendimientos económicos sino cubrir sus necesidades operativas.

⁸ NIKOS PASSAS y ANDREA GIMÉNEZ-SALINAS FRAMIS, «La financiación del terrorismo de Al Qaeda: mitos y realidades». *Inteligencia y Seguridad. Revista de Análisis y Prospectiva*, nº 2, septiembre 2007, pp. 47-78. esp. p. 52.

⁹ RÜDNER, «Hizbullah Terrorism Finance...», *cit.* p. 711.

¹⁰ MIKEL FREEMAN, «Sources of Terrorism Financing: Theory and Typology». En MIKEL FREEMAN (ed): *Financing Terrorism: Case Studies*. Surrey: Ashgate e-Book, 2012.

b) La legitimidad de las fuentes de financiación

Este criterio es importante debido a que las organizaciones terroristas tienen naturaleza política por lo que todas sus acciones, deben de ser legítimas a los ojos de la sociedad o de la población en cuyo nombre actúan buscarán ser legitimadas ante la sociedad o la población en cuyo nombre actúan. Por lo tanto, no podrán responsabilizarse de la realización de actos ilegítimos como pueden ser el narcotráfico o el secuestro, ya que esto los deslegitimaría ante sus seguidores.

c) La seguridad

Es un punto clave dado que las organizaciones terroristas asumen riesgos en sus acciones, especialmente para obtener beneficios, por lo que será crucial para su éxito el ocultarse de las fuerzas de seguridad del Estado.

d) A fiabilidad de las fuentes de financiación

Las organizaciones terroristas tratarán de explotar aquellas que sean predecibles y ofrezcan un flujo regular de recursos, apartándose por el contrario de aquellas que estén sujetas a fluctuaciones aleatorias o a casuísticas que les impidan una obtención de recursos rápida y fácil.

e) La simplicidad

Los métodos de obtención de recursos utilizados por la organizaciones terroristas deben ser sencillos, obtenidos con poco esfuerzo y a ser posible con un coste reducido. Todo ello les permitirá rentabilizar las operaciones que lleven a cabo sus militantes frente a acciones que requieran una alta cualificación, una operativa compleja o tengan un coste elevado. Así por ejemplo, hay organizaciones que utilizan las redes sociales y el *crowdfunding* para conseguir financiación por tener un carácter anónimo que mueve pequeñas cantidades, lo que dificulta su identificación y seguimiento. Otras organizaciones benéficas emplean las redes de remesas o *hawala*, que es un sistema de transacciones informal¹¹

¹¹ Las redes *hawala* son uno de los servicios financieros más usados y existen en todo Oriente Medio, el Norte de África y el sur y sudeste de Asia.

utilizado especialmente para las comunidades que se encuentran expatriadas de sus familias en sus países de origen. Especialmente las redes *hawala* plantean importantes problemas para los servicios de inteligencia y las fuerzas y cuerpos de seguridad a la hora de descubrir sus finalidades ilícitas.

Junto a la *hawala*, también existen otros sistemas informales de transferencia de fondos que operan de forma similar y que son utilizado por la población de forma legítima sin dejar rastro de dichas transacciones, son entre otros las siguientes:

Hundi es uno de los instrumentos de crédito más importantes de la India, que toma su base de las operaciones financieras europeas de los siglos XII y XIII. El mercado negro del peso y otras redes de cambio también se utiliza como forma de financiación, siendo *el Fei chien* una variante asiática con características similares a las anteriores.

Todos estos sistemas están activos en muchos países y constituyen una forma de pago muy utilizada para todos aquellos que desean realizar transferencias, tanto legales como ilegales a las organizaciones terroristas. Lo que los hace atractivos para la población es tanto su eficacia, como la posibilidad de acceso a lugares remotos y subdesarrollados, el anonimato o su bajo coste entre otros.

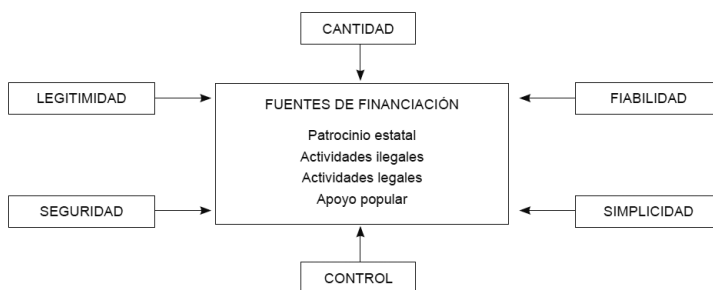
f) El control

Dada la naturaleza política de las mayoría de las organizaciones terroristas, es fundamental operar en la clandestinidad fuera del alcance de los sistemas de seguridad impuestos por los Estados. Por otro lado, estos grupos intentan controlar al máximo sus fuentes de recursos para evitar de este modo filtraciones que puedan poner en peligro sus estructuras.

A partir de los criterios creados por Freedman, Buesa ha elaborado un cuadro donde se pueden contemplar como quedan contenidos los elementos que manejan las organizaciones terroristas para establecer sus fuentes de financiación.

Una vez establecida la clasificación de las formas de financiación de manera global y la variedad de criterios a los que se puede acudir para identificar las preferencias en la obtención de ingresos, se pueden enumerar diferentes tipos de operaciones de captación de fondos teniendo en cuenta su evolución así como el carácter legal o ilegal de su fuente.

ESQUEMA 1
FUENTES DE FINANCIACIÓN DEL TERRORISMO Y SUS FACTORES DETERMINANTES



FUENTE: Elaborado a partir de FREEMAN (2012).

3. El origen de las fuentes de financiación: entre la legalidad y la ilegalidad

Identificadas las fuentes de financiación que sustentan la estructura y actividades de los grupos terroristas, hay que diferenciar la financiación del terrorismo de otras formas irregulares de utilización del sistema financiero. Según Passas y Giménez¹², es el hecho de que los fondos utilizados por los terroristas sea legal lo que diferencia el concepto de financiación del terrorismo de otros conceptos como el blanqueo de capitales.

De hecho, las operaciones de blanqueo de capitales siempre parten de un origen ilegal de los fondos, siendo necesario utilizar diferentes para volver a introducir el dinero dentro del sistema financiero legal. Sin embargo, en la financiación del terrorismo, el origen de los fondos puede ser legal, por ejemplo, utilizando criptomonedas, no siendo necesario el blanqueo de dinero si los fondos van a ser utilizados directamente para financiar un atentado. En estos casos, la financiación del terrorismo y el blanqueo de capitales funcionan a la inversa, es decir, un dinero de procedencia legal es utilizado para fines ilegales. Por otro lado, si los fondos son de procedencia ilegal, no es necesario su blanqueo ya que su finalidad será ilegal y por tanto lo único que hay que hacer es ocultarlo para que no puedan ser rastreado por las fuerzas de seguridad.

¹² PASSAS, GIMÉNEZ-SALINAS FRAMIS, «La financiación el terrorismo...», *cit.* p. 497.

Como consecuencia de este doble origen la financiación terrorista abarca un amplio abanico de actividades financieras que va desde la logística y la financiación de actividades que ayudan a mantener las infraestructuras terroristas, hasta los aspectos operativos que dependen de los objetivos, el *modus operandi* y la magnitud de las operaciones terroristas.

Un informe de 2015 del Grupo de Acción Financiera (FATF por sus siglas en inglés) identificaba la presencia de cinco fuentes principales de ingresos: las ganancias ilícitas obtenidas por la ocupación del territorio (saqueo de bancos, extorsión, control de los campos petrolíferos y de las refinerías, impuestos ilícitos sobre bienes y productos y sobre el dinero que circula por el territorio en el que opera el EI); los rescates de secuestros; las donaciones, incluidas las de organizaciones sin ánimo lucro o conseguidas a través de estas organizaciones; la ayuda material de los combatientes terroristas extranjeros (FTF por sus siglas en inglés); y la recaudación de fondos mediante redes de comunicación modernas (FATF, *Financing of the Terrorist Organisation Islamic State*)¹³.

3.1. Las fuentes de financiación de origen ilegal de los grupos terroristas

La financiación por parte de grupos terroristas ha evolucionado a lo largo de los años por lo que se puede decir que si bien en un primer momento las fuentes tuvieron exclusivamente un origen ilegal, con el tiempo y de la mano de la digitalización de la sociedad se ha virado hacia fuentes de origen legal que devienen ilegales por el fin para el que son utilizados dichos fondos. Esto no quiere decir que se hayan abandonado las primeras, por el contrario, ambas formas conviven siendo utilizadas en función del territorio y del acceso a las tecnologías que se manejen.

Entre las formas más habituales de financiación ilegal destacan las siguientes:

¹³ MAGNUS RANSTORP, «La financiación del terrorismo: principales actores, estrategias y fuentes», *Afkar Ideas*, primavera 2018. pp. 52-55, esp. p. 52.

a) Lavado de Dinero

Las organizaciones terroristas pueden utilizar esquemas de lavado de dinero para ocultar el origen ilegal de los fondos. Esto implica la manipulación de transacciones financieras para hacer que los fondos parezcan legítimos¹⁴.

b) Tráfico de drogas

Determinados grupos terroristas utilizan para obtener una financiación fácil y segura su asociación con el narcotráfico participando bien sea con el control de las rutas de contrabando o con operaciones relacionadas con la producción y distribución de drogas ilegales. Por ejemplo, las ganancias obtenidas con el tráfico de drogas pudieron ser identificadas en los atentados de Madrid (2004), el grupo *Hofstadt*(2004), el caso de *Mohamed Merah* (2012) y el de *Anis Amri*, el atacante de Berlín (2016) que no solo vendía drogas, sino que también las consumía. Según Europol, las investigaciones de los atentados terroristas en Bruselas (2016) y París (2015) revelaron que algunos de los autores de estos atentados estaban implicados en el tráfico ilegal de drogas y mantenían contactos con grupos criminales implicados en el tráfico de armas y en la elaboración de documentos falsos¹⁵. Así mismo, entre las fuentes de ingresos de *Hezbollah* se incluyen las actividades de blanqueo de dinero y de tráfico de drogas en todo el mundo, ya que su extensa red se extiende por África, Centroamérica y Sudamérica.

c) Secuestros, Extorsiones y Trafico de personas

Los grupos terroristas pueden financiarse mediante secuestros con el objetivo de obtener rescates. También pueden recurrir a la extorsión amenazando

¹⁴ PIERRE LAURENT CHATAIN et al., «Integrity in Mobile Phone Financial Services: Measures for Mitigating the Risks from Money Laundering and Terrorist Financing», *The World Bank*, 2008 <https://doi.org/10.1596/978-0-8213-7556-3>. NAVIN BEEKARRY, «International Anti-Money Laundering and Combating the Financing of Terrorism Regulatory Strategy: A Critical Analysis of Compliance Determinants in International Law». *Nw. J. Int'l L. & Bus* n° 31, 2011, p. 137.

¹⁵ RANSTORP, «La financiación del terrorismo...», cit. p. 52.

a individuos o empresas para obtener dinero. El tráfico de inmigrantes o la inmigración ilegal parece que ha sido también un recurso utilizado por grupos terroristas para procurar financiación a sus miembros.

d) Financiación extranjera ilícita especialmente por parte de Estados extranjeros

Recibir fondos de fuentes extranjeras, a menudo a través de redes clandestinas, para llevar a cabo actividades terroristas es otra forma ilegal de financiamiento. Es el caso de la financiación a grupos terroristas por parte de Estados extranjeros que consiguen con ello controlar a estos grupos asegurando así que cumplirán con los objetivos políticos que persiguen. Por ejemplo, el papel de la financiación por parte de Irán del grupo libanés *Hezbollah* está bien documentado. Otra fuente de financiación estatal a grupos terroristas *takfiríes-salafistas* procede de los Estados del Golfo, que proporcionan apoyo ideológico y financiero en todo el mundo. En este sentido, el papel de Arabia Saudí para promocionar su ideología wahabí, que se difunde a través de fundaciones benéficas paralelas que prestan un generoso apoyo financiero para construir mezquitas con una orientación wahabí, está bien documentado. También se ha acusado a Catar y Kuwait de financiar al *ISIS* y a grupos extremistas yihadistas en todo Oriente Medio y en otros lugares. Se trata por tanto de extender su poder de una manera global trasladando los enfrentamientos entre suníes y chiíes al contexto geopolítico internacional¹⁶.

e) Robo y Asalto

Algunas organizaciones terroristas participan para obtener fondos en actividades criminales directas, como robos a mano armada. Los terroristas aprovechan para llevar a cabo estas acciones documentos de viaje falsos, la accesibilidad a las armas en las bandas callejeras, las redes de traficantes y los pisos francos para moverse sin ser detectados. De este modo consiguen acceder a las bandas criminales tejiendo redes para mejorar su operatividad.

¹⁶ *Ibidem* p. 55.

Recordar que dentro de la organización Al Qaeda había un grupo de personas, casi todas de origen argelino, expertas en la falsificación de pasaportes

f) Fraude y Delitos Financieros

Participar en fraudes financieros, como estafas, falsificación y manipulación del sistema financiero es otra manera en que los grupos terroristas pueden obtener recursos.

g) Donaciones Falsas y Organizaciones Caritativas Ilegales¹⁷

Algunos grupos terroristas han utilizado organizaciones caritativas falsas o mal gestionadas para disfrazar la transferencia de fondos. En estos casos la finalidad de las donaciones recibidas pueden destinarse a actividades terroristas en lugar de obras a benéficas legítimas.

En el terrorismo islámico es el caso de *La Zakat* que es uno de los cinco pilares del islam y se refiere a la obligación de dar limosna o caridad por parte de los musulmanes que tienen la capacidad financiera de hacerlo. Es un acto de adoración y una forma de redistribución de la riqueza en la comunidad islámica. La cantidad exacta es el 2,5% de la riqueza total acumulada, y este porcentaje se aplica a diversas formas de riqueza, como dinero en efectivo, bienes raíces, joyas y otros activos comerciales. La palabra «Zakat» proviene de la raíz árabe que significa «purificación» y «crecimiento». Además de las donaciones *zakat*, que son obligatorias, existen también las donaciones voluntarias como el *infaq* y *shadaqah* que se efectúan en ocasiones concretas.

El problema de las organizaciones benéficas y su posible relación con la financiación del terrorismo siempre ha sido difícil de controlar para los gobiernos occidentales, por lo que como consecuencia de ello muchas organizaciones benéficas sufren retrasos en las transacciones, denegaciones o cierres de cuentas por parte de los bancos debido a la sospecha de que puedan estar llevando a cabo actividades ilegales de financiación del terrorismo. Para evitar situaciones injustas, los gobiernos y las instituciones financieras han desarrollado los llamados «indicadores de bandera roja» a través de los cuales

¹⁷ PASSAS, GIMÉNEZ-SALINAS, «La financiación el terrorismo...», cit. p. 509.

intentan detectar y minimizar el riesgo de que las organizaciones benéficas financien el terrorismo usando empresas falsas o bancos «pantalla», cuentas bancarias extranjeras o la utilización de fondos personales para confundir a las instituciones que controlan la legalidad de las transacciones.

Por otro lado, en la aportación de contribuciones benéficas a las organizaciones terroristas que cuentan con actividades militares, sociales y políticas resulta difícil distinguir dónde empieza una parte de la organización y dónde acaba otra. Esto ha dado lugar a confusión en los juicios que se llevan a cabo cuando se perpetran atentados terroristas, de tal forma que por ejemplo, solo la rama militar de *Hezbollah*, y no el resto de la organización militante chií, aparece en la lista de organizaciones terroristas de la Unión Europea.

h) La Red profunda y la Red oscura

La *Deep Web* o «Red Profunda» se refiere aquella parte de la Web que no está indexada por los motores de búsqueda tradicionales como pueden ser Google o Yahoo, siendo muy difícil de rastrear, y estando, muchos de los contenidos que allí se contienen protegidos por mecanismos de seguridad tales como logins de identificación, contraseñas, etc.¹⁸

Por otro lado, la *Dark Web*, o «Red oscura», sirve para referirse a aquellos sitios o páginas contenidos en las redes anónimas¹⁹, refiriéndose a aquellas tecnologías de red que permitían distribuir contenido digital utilizando una red física subyacente sobre la que implementar una aplicación o capa de protocolos de comunicación. Dicho de otro modo, se trataba de añadir la necesidad de privacidad permitiendo la transferencia de información sin que la identidad de los intervinientes o el contenido pudiese ser conocida. No obstante estos contenidos son accesibles a cualquier usuario mediante el empleo de *proxies* o de navegadores específicos diseñados para tal fin, proporcionando su uso anónimo tanto para el usuario que trata de acceder a la información, como para el que lo publicó²⁰.

¹⁸ MIKEL BERGMAN, «The Deep Web: surfacing hidden value», 2001. <http://grids.ucs.indiana.edu/courses/xinformatics/searchindik/deepwebwhitepaper.pdf> (consultado el 12 de enero de 2024).

¹⁹ El término lo crearon investigadores de la empresa informática Microsoft.

²⁰ CARLOS YUSTE GONZÁLEZ, *Deep web y monedas virtuales: entorno privilegiado para las organizaciones terroristas*, Trabajo Fin de Master (inérito), Universidad de la Rioja, 2015, p.7 .

También habría que hacer mención a una clasificación que se ha desarrollado sobre distintos niveles de profundidad en base al tipo de contenidos y la gravedad o ilegalidad de los mismos, pudiendo tener su importancia desde el punto de vista policial o judicial, ya que a mayor profundidad los contenidos serán más graves.²¹

Es compleja la elaboración, a priori, de una correlación de usos que dichas organizaciones estén haciendo de este medio, debido, en parte, a la propia idiosincrasia del medio ya que la información existente sólo se puede encontrar en fuentes cerradas con nivel alto de clasificación, lo cual, indudablemente es imposible de probar al no poder acceso al contenido.

En este sentido, la ONU publicó un documento 2013, elaborado, en concreto, por la Oficina de las Naciones Unidas contra la Droga y el Delito (UNODC) en colaboración con el Equipo Especial sobre la Ejecución de la Lucha contra el Terrorismo, titulado «El uso de internet con fines terroristas». A través de este documento se puede comprobar la dimensión de Internet en la difusión y financiación del terrorismo.

En un principio, los grupos terroristas crearon sus propios sitios web de carácter oficial, pero tras el 11-S fueron perseguidos, tanto por los servicios de inteligencia como por la comunidad hacker, lo cual les obligo a un constante cambio en la red en busca de alojamientos y dominios que los

²¹ Así tendríamos los siguientes niveles: Nivel 1. *Surface Web*. Correspondería con la *Web* superficial en la que navega la mayoría de los usuarios y en la que se sitúan sitios web Google, Facebook, etc. Nivel 2. *Bergie Web*. Se corresponde con la *Web* superficial, pero con unos contenidos que ya sí serían, en algunos casos, ilegales. Se encontrarían por ejemplo páginas con contenido pornográfico, o aquellas que violan derechos de propiedad intelectual como pueden ser servicios de televisión en *streaming*. Nivel 3. *Deep Web*. Este nivel requiere el empleo de un *proxy* de cara a preservar el anonimato. Entre los contenidos que se pueden encontrar en este nivel destacaría la pornografía infantil, la venta de sustancias estupefacientes o el proselitismo del terrorismo islámico. Nivel 4. *Charter Web*. Se necesita el uso de *Tor* para navegar en este nivel (*Tor* es un *software* libre multiplataforma que implementa una red de comunicaciones distribuida, cifrada, de baja latencia y superpuesta a internet. En ella el enrutamiento de paquetes se realiza ocultando la dirección IP de los usuarios logrando así el anonimato en la capa IP o de red). Se pueden encontrar los foros *underground*, en los que se pueden adquirir sustancias estupefacientes, armas, o contratar servicios criminales denegación de servicio, o la compra de tarjetas falsas entre otros. Nivel 5. *Marianas Web*. Su contenido es muy restringido y, normalmente, de origen ilícito pero de extrema gravedad como pueden ser delitos de terrorismo, trata de seres humanos, etc. Ver YUSTE GONZÁLEZ, *Deep web* y monedas virtuales..., cit. p. 4.

sacó del sistema²². En esos momentos, además, era muy difícil mantener un dominio debido a que la contratación de debía hacer con cargo a una tarjeta de crédito lo cual delataría la identidad del pagador. Posteriormente optaron por el pago de tarjetas robadas, pero una vez el fraude era descubierto el servicio quedaba cancelado. En la actualidad esos problemas los pueden solventar los terroristas con facilidad acudiendo a las posibilidades que la *dark web* les brinda: emplean una identidad falsa adquirida en un *dark market*, y buscaran empresas que presten ese servicio y admitan el pago en bitcoins, como *digitalvalley*, *namecheap*, *allwebs.host*, etc., lo que adelante, garantizará el total anonimato de quien realiza el pago.

Respecto al reclutamiento, la radicalización y la incitación al terrorismo todos ellos encuentran un lugar propicio en el uso de salas chat o de foros en la *deep web* utilizando sus servicios en total anonimato (proporcionada por la red *TOR*), con una estructura similar, en cuanto a jerarquía, a la de los foros tradicionales que se pueden encontrar en la *surface web*: administradores, moderadores y usuarios comunes. En algún foro el acceso se haría, exclusivamente, por invitación de algún individuo que ya estuviese integrado en el mismo y con cierta reputación, poniendo ésta como garantía y aval para que el nuevo miembro fuese admitido, siendo un buen método para limitar la posible infiltración.

Otro de los espacios ocupados en la *deep web* por parte de las organizaciones terroristas es la de obtención de financiación a través de la petición de fondos para sufragar sus actividades. La recaudación directa se realiza utilizando sitios web y foros, comunicaciones directas a los posibles simpatizantes en las que se les solicitaría una donación, etc. En un principio, los sitios web o foros admitían que la transferencia de los fondos se realizasen por medio de transferencias electrónicas, sin embargo, en la actualidad, optan por solicitar los donativos con bitcoin para asegurar así el anonimato.

i) El *Black market* o Mercado negro

La descentralización y fragmentación de muchas organizaciones terroristas, particularmente de Al Qaeda, trajo consigo la necesidad de que las células

²² MANUEL TORRES SORIANO, «Terrorismo yihadista y nuevos usos de Internet: la distribución de propaganda». Real Instituto Elcano. ARI nº 110, 2009.

locales tuvieran que autoabastecerse para llevar a cabo los atentados terroristas. Para evitar ser descubiertos por los cuerpos de seguridad en el tráfico de sustancias estupefacientes a pequeña escala que les reportaban fondos fáciles y rápidos, comenzaron a utilizar Internet, a través de denominado *black markets* que está ubicado en la *dark web*, y, muy especialmente, en *Tor*.

En estos mercados se puede adquirir prácticamente cualquier producto considerado ilegal, como puede ser la adquisición de sustancias estupefacientes, armas de fuego, documentos de identidad falsos, servicios de *hacking*, servicio de sicarios entre otros. En definitiva, se podría tener acceso a servicios criminales contratando los servicios en la red y pagando en bitcoins «*crime as a service*».

3.2. Las fuentes de financiación de origen legal de los grupos terroristas

El hecho de que los grupos terroristas utilicen fuentes de financiación pensadas para sufragar proyectos legales para costear atentados terroristas no justifica su origen, por el contrario, deberían estar más cuestionados ya que generan desconfianza tanto en las instituciones como en la sociedad impidiendo que estos sistemas puedan ser utilizados tanto por la ciudadanía como en operaciones comerciales de carácter global.

Una de las características de estas fuentes de financiación está relacionada con el uso de la tecnología a través de herramientas digitales. Estos sistemas permiten ocultar operaciones que pueden cruzar el mundo en milésimas de segundo transfiriendo pequeñas cantidades de dinero difícilmente detectables por las instituciones de control. También permiten enviar información camuflada en mensajes cifrados que mantienen el anonimato de las fuentes.

Todo ello está obligando a la sofisticación de los medios de control naciendo así la llamada ciberguerra²³ en la que las armas son sustituidas por los ordenadores que se han convertido en el campo de batalla de los ataques terroristas del Siglo XXI.

²³ BORJA GARCÍA VÁZQUEZ, «El derecho internacional frente a los nuevos medios y espacios en que desarrollar la guerra: La ciberguerra», *Revista Chilena de Derecho y Tecnología*, vol.10 n° 2, 2021, pp. 1-27; y FRANCISCO UREÑA CENTENO, «Ciberataques, la mayor amenaza actual», *IEES*, n° 9, 2015 pp. 1-18.

A continuación se pasará a enumerar las principales fuentes de financiación que operan en la financiación de grupos terroristas.

3.2.1. Uso de Internet para difundir propaganda y recaudar fondos

Por un lado la *Web* se ha utilizado para promover la ideología extrema y la violencia, teniendo como resultado el incremento exponencial, a nivel mundial, de las personas que pueden ser receptoras de dicho mensaje. A ellos se une la posibilidad de que sean los propios grupos terroristas quienes distribuyan directamente el contenido de sus mensajes a través de Internet, lo que les ofrece una elevada independencia de los medios o canales tradicionales de comunicación. Incluso han llegado a ser los medios de comunicación quienes se habrían interesado por reproducir videos subidos por los terroristas.

Éstos han optado por el empleo de plataformas de redes sociales con una implantación masiva como Twitter y Facebook, como medio para distribuir su mensaje y conseguir captar nuevos seguidores. Una vez han conseguido nuevos adeptos suelen contactar con ellos por medio de mensajería instantánea como *WhatsApp* para, posteriormente y si se comprueba que la evolución ideológica y posibilidades de radicalización son positivas, llegar al contacto directo. Por otro lado han procurado el empleo de sitios web muy populares como puede ser *Youtube* para poder subir videos propagandísticos, además del empleo de empresas que ofrecen servicios web de alojamiento de archivos de gran tamaño, como puede ser *RapidShare* o *Mega*.²⁴

Igualmente, Internet se ha revelado como un canal muy importante para la obtención de fondos económicos con los que financiar a grupos y células, o, directamente, actos de terrorismo. La UNODC afirma que los terroristas pueden recurrir a la recaudación de fondos y recursos en Internet de acuerdo a cuatro categorías: recaudación directa; comercio electrónico; empleo de los servicios de pago en línea y contribuciones a organizaciones benéficas.

²⁴ YUSTE GONZÁLEZ, *Deep web y monedas virtuales...*, op. cit. p.18.

3.2.2. Microfinanciación

La microfinanciación es básicamente una herramienta destinada a proporcionar servicios financieros a personas de bajos ingresos, especialmente aquellos que no tienen acceso a servicios bancarios tradicionales. Estos servicios incluyen pequeños préstamos, ahorros y seguros. Estas características han convertido este sistema de captación de fondos en una herramienta muy útil para empoderar a comunidades marginadas fomentando el emprendimiento y el desarrollo económico en áreas desfavorecidas²⁵.

Sin embargo, estas mismas peculiaridades son las que han utilizado los grupos terroristas para financiar sus actividades ilícitas ya que al ser pequeñas cantidades de dinero lo que se recauda no da lugar a sospechas. Así por ejemplo, la rápida expansión de los “lobos solitarios” o los pequeños grupos autónomos que emplean un *modus operandi* terrorista sencillo, con costes operativos muy bajos y con resultados muy eficaces como son los ataques con camiones o con cuchillos. Estos atentados se financian con este tipo de envíos que resultan muy difíciles de detectar por parte de las fuerzas antiterroristas. Las operaciones a través de la que se llevan a cabo estas acciones revisten las siguientes formas:

- a) Penetración en instituciones microfinancieras infiltrándose los grupos terroristas en estas estructuras o estableciendo sus propias oficinas bajo la apariencia de programas de desarrollo utilizando estos canales para canalizar fondos ilícitos;
- b) Apropiación de recursos financieros locales en áreas donde la microfinanciación es una herramienta vital para el desarrollo comunitario intentando apropiarse de recursos financieros locales mediante la intimidación, la extorsión o la coacción;
- c) Uso de actividades empresariales aparentemente legítimas, como pequeños negocios o proyectos agrícolas, para canalizar fondos ilícitos bajo la apariencia de microfinanciación;
- d) Abuso en el uso de programas de desarrollo con el desvío de fondos destinados a actividades legítimas hacia actividades ilícitas;

²⁵ MANUEL CARLOS JIMÉNEZ CASTILLO, *Economía del desarrollo humano y microfinanciación: Una aproximación a los determinantes de microcrédito*. (Tesis Doctoral Inédita). Universidad de Sevilla, Sevilla, 2013; y CARMEN PARRA RODRIGUEZ, *Empresas con conciencia*, Editorial Viceversa, Barcelona, 2010.

- e) Extorsión a emprendedores locales en entornos donde la microfinanciación está destinada a respaldar pequeños negocios locales utilizándolos para la extorsión o la intimidación obligando a los emprendedores a proporcionarles una parte de sus ganancias.

Es fundamental destacar que estas prácticas son ilegales y violan los principios fundamentales de la microfinanciación que nació con la finalidad de mejorar las condiciones de vida de las comunidades desfavorecidas. En este sentido, dos estudios de la Universidad de Defensa Sueca de 2017 sobre las actividades de financiación de los FTF suecos mostraron que muchos de ellos habían recibido ayudas sociales o microcréditos bancarios. A pesar de esta apariencia de legalidad muchos de ellos habían perpetrado fraudes financieros, a través de créditos por SMS, fraude en la recaudación del IVA y recaudación de dinero a través de organizaciones benéficas o del *crowdfunding*²⁶.

Para evitar estas actividades ilegales las instituciones de microfinanciación y las organizaciones internacionales trabajan en estrecha colaboración para implementar medidas de control que reduzcan los riesgos que esta actividad produce, asegurándose de que los servicios financieros se utilicen de manera ética y para que el beneficio obtenido sirva para sufragar los verdaderos fines para los que han sido creados. La regulación y supervisión adecuadas son esenciales para prevenir la explotación de la microfinanciación con fines ilícitos.

Así por ejemplo conocer los métodos de microfinanciación de los FTF proporciona una información inestimable sobre las conexiones financieras, las estructuras de las redes y las líneas de abastecimiento logísticas. La identificación de estas conexiones permite a los servicios de inteligencia entender mejor los nodos y los vínculos operativos fundamentales entre los diferentes grupos terroristas. Todo ello requiere una mayor coordinación entre los servicios secretos, las fuerzas y cuerpos de seguridad del Estado y las instituciones financieras. A pesar de ellos, en el caso del *ISIS* no ha resultado fácil seguir los flujos financieros de los FTF, especialmente porque las transferencias se han realizado a bancos turcos y a oficinas de cambio en el Sur de Turquía, en la frontera con Siria.

²⁶ RANSTORP, «La financiación del terrorismo...», p. 53.

3.2.3. Monedas virtuales

Otra de las prioridades de los servicios de inteligencia es centrarse en entender la manera en que las nuevas tecnologías influyen en los métodos terroristas en los que se usan comunicaciones seguras y nuevas técnicas para transferir fondos anónimamente a través de las fronteras.

Las monedas virtuales o criptomonedas son un sistema de pago a través de Internet, basadas en un sistema *peer-to-peer* (P2P o red entre iguales), que contienen un elemento de seguridad basado en la criptografía y en donde el valor es transmitido electrónicamente entre las partes sin un intermediario. Las monedas virtuales operan como una moneda en un medio determinado (*Internet*), pero a diferencia de las monedas reales no tienen una base legal que las ligue a un control por parte del Estado, no tienen forma física en billetes o monedas, siendo identificadas por contar con una cadena de caracteres digitales.

Entre las características de este tipo de monedas se pueden destacar están el anonimato. En este sentido no se requiere que las partes prueben su identidad y tenga que ser verificada y validada, no siendo necesario aportar datos sobre la identidad de los participantes en la transacción económica. Su alcance global, la rapidez en su transferencia, la no posibilidad de rechazo, un bajo coste (sin pago de comisiones), facilidad en su uso, complejidad en seguir el rastro de las operaciones, y carece de regulación nacional o internacional. Todo ello las sitúa en un sistema de captación de fondos ideal para los grupos terroristas.

De las monedas virtuales el *bitcoin* es una de las más populares, entendida como una red consensuada que permite un nuevo sistema de pago y una moneda completamente digital. Esta moneda electrónica, junto a un *software* y un protocolo, permite la realización de transacciones casi instantáneas entre iguales, ya que se basa en el sistema *peer-to-peer* (P2P). A través de este sistema se pueden hacer pagos a nivel mundial con unos costes nulos o muy pequeños al realizar dichas transacciones. Por otro lado, al operar bajo la tecnología *peer-to-peer* evita depender de una autoridad monetaria central que sería la responsable de la emisión y el control del dinero, siendo, por tanto, un sistema completamente privado²⁷.

²⁷ SATOSHI NAKAMOTO INSITUTE, «Bitcoin open source implementation of P2P currency», 2009, <http://p2pfoundation.ning.com/forum/topics/bitcoin-open-source> (consultado 10 enero 2024); ver también www.bitcoin.org.

Para asegurar su seguridad emplea la criptografía garantizando así que las transacciones de cada *bitcoin* y cada usuario estén encriptados con un único identificador, quedando cada transacción registrada y grabada en una especie de libro de contabilidad, conocido como *blockchain*, que puede ser visto por cualquier usuario de la red, pero que no revela ningún dato personal acerca de las partes que realizaron la transacción económica²⁸.

Todo ello hace sospechar a las agencias de inteligencia que los grupos terroristas, el *ISIS* entre otros, emplean las criptomonedas para transferir dinero a sus operativos en occidente. Así por ejemplo, hay indicios de que la limosna que los buenos musulmanes deben dar a favor de la lucha se están haciendo en bitcoins para evitar los controles que los Estados *kafir* imponen en el sistema financiero ordinario, sugiriendo el empleo de la *dark wallet* permite un total anonimato²⁹.

Llegados a este punto habría que distinguir entre la utilidad de esta moneda para organizaciones terroristas como el *ISIS* o *Hezbollah*, y su empleo por parte de células locales. Con respecto al empleo del *bitcoin* por parte de grupos terroristas que controlan un amplio territorio buscando la creación de una estructura de Estado, el uso del bitcoin no es una buena opción ya que este tipo de organizaciones necesitan grandes cantidades de dinero que en el caso del *ISIS* consigue a través del control de los pozos de petróleo que vende en los circuitos de mercado negro tradicionales proporcionándoles grandes ingresos de dinero, a lo que habría que sumar el dinero que obtiene producto del pago de rescates por los secuestros de occidentales y de la venta de las antigüedades que expolían del patrimonio histórico de los lugares que controlan.

Por el contrario, el uso del bitcoin por parte de células locales está más indicado ya que las condiciones que reúnen (anonimato, inmediatez, ausencia de fronteras y controles legales entre otros), facilitan el envío de dinero a operativos que estén radicados clandestinamente en países occidentales o, en sentido contrario, enviar dinero captado en Occidente a las zonas de

²⁸ Instituto Nacional de Ciberseguridad INCIBE, «Bitcoin. Una moneda criptográfica», 2014, https://www.incibe.es/CERT/guias_estudios/Estudios/bitcoin_moneda_criptografica.

²⁹ Ver «Bitcoin wa Sadaqat al-Jihad» (Bitcoin y la limosna de la lucha física violenta, disponible en <https://alkhilafaharidat.files.wordpress.com/2014/07/btcredit-21.pdf>. (consultado el 12 de enero de 2024).

conflicto, haciendo, casi imposible, a las autoridades locales su localización y monitorización. Según dice Yuste, «estos individuos sí harían uso de ese dinero virtual para obtener productos, como armas y explosivos, en los *black markets*, o para contratar servicios de hacking, pudiendo éstos ser transferidos por el propio *ISIS* u otra matriz de organización terrorista, bien como producto de donativos recibidos de todas las partes del mundo, o bien obtenidos directamente por ellos mediante el uso fraudulento de numeraciones de tarjetas de crédito, además de otras posibilidades que les facilitan los *black markets*, haciendo de estos sitios en *Internet* y del *bitcoin* elementos básicos para la financiación de las células terroristas»³⁰. También estas células locales pueden adquirir productos cotidianos en los comercios que aceptan como medio de pago criptomonedas con conversión a su moneda local.

3.2.4. Tarjetas de prepago

Las tarjetas de prepago de uso múltiple tienen utilidades legítimas y son un instrumento que contribuye a la inclusión social y financiera. No obstante, las tarjetas de prepago anónimas son fáciles de utilizar para financiar la logística y los atentados terroristas. Resulta por lo tanto esencial privar a los terroristas de ese medio de financiación en sus operaciones, reduciendo los límites y los importes máximos por debajo de los cuales se autoriza a las entidades obligadas a no aplicar algunas de las medidas de diligencia debida identificando al consumidor en caso de operaciones remotas de pago cuyo importe sea superior a 50 EUR.

Esto se refiere no solo a las comunicaciones seguras mediante aplicaciones de redes sociales encriptadas, sino también a los métodos innovadores para no ser detectados por los servicios de inteligencia y las fuerzas y cuerpos de seguridad. Por ejemplo, los terroristas utilizaron tarjetas de prepago para preparar los atentados de París en noviembre de 2015 y así no ser identificados. Los atacantes de París también tenían un gran número de teléfonos desechables y usaban redes sociales encriptadas para comunicarse. Rahmat Akilov, el terrorista que perpetró el ataque con un camión en el centro de Estocolmo en abril de 2017, también empleó otro modus operandi terrorista innovador:

³⁰ YUSTE GONZÁLEZ, *Deep web y monedas virtuales...*, op. cit. p. 43.

utilizó las redes sociales rusas Odnoklassniki y VKontakte y suministró 53 tarjetas SIM de prepago anónimas sus contactos del EI en Siria que le ayudaron a registrarse en *Whatsapp*³¹.

En este sentido se ha criticado que el uso de tarjetas de prepago anónimas emitidas en la UE se limite básicamente a este territorio, obviando las tarjetas similares emitidas en terceros países. Es por lo tanto importante asegurar que las tarjetas de prepago anónimas emitidas fuera de la UE solo puedan utilizarse en el espacio europeo si cumplen los requisitos equivalentes a los establecidos en Derecho de la UE.

3.2.5. Fideicomisos (del tipo *trust*)

El fideicomiso, también conocido como *trust* en inglés, es un negocio legal por el cual una persona (llamada fideicomitente) coloca su propiedad y activos en manos de otra persona o entidad (llamada fiduciario) para el beneficio de otra persona o grupo de personas (llamados beneficiarios). Este instrumento legal se utiliza con diversos propósitos, incluyendo la financiación de proyectos específicos o para asegurar la gestión y distribución de activos de manera planificada³².

Es importante destacar que los fideicomisos se utilizan comúnmente con fines legítimos y legales, como la planificación patrimonial, la protección de activos y la gestión de inversiones. Sin embargo, en la actualidad se utilizan con la intención de financiar actividades ilegales, como el terrorismo, el blanqueo de capitales, o delitos subyacentes conexos³³.

En este sentido, los riesgos de blanqueo de capitales y financiación del terrorismo que ello implica pueden diferir, en función de las características del tipo de fideicomiso (del tipo *trust*) o por un instrumento jurídico análogo, pudiendo evolucionar los riesgos que ello conlleva en función de la evolución de tiempo, por ejemplo como consecuencia de las evaluaciones

³¹ RANSTORP, «La financiación del terrorismo...», p. 54.

³² NICOLÁS FONT, «Trust in the European Union in challenging times». *Relaciones internacionales*, 28(56), 2019, pp. 285-287 (consultado el 17 de enero de 2024), http://www.scielo.org.ar/scielo.php?script=sci_arttext&pid=S2314-27662019000100024&lng=es&tlng=es.

³³ BASIA SPALEK, «Community Policing, Trust, and Muslim Communities in Relation to “New Terrorism”», *Politics Policy*, vol. 38, issue 4, 2010, pp. 653-886.

de los riesgos a nivel nacional y supranacional. Por otro lado, a la hora de determinar el nivel de transparencia de la información relativa a la titularidad real de tales fideicomisos o instrumentos jurídicos análogos, los Estados deben tener en cuenta la protección de los derechos fundamentales de las personas físicas, en particular el derecho a la intimidad y la protección de sus datos personales.

4. El papel de las instituciones internacionales en la lucha contra la financiación del terrorismo

El hecho de que todos estos sistemas de captación de recursos se utilicen en la actualidad con cierta impunidad se debe a que no existen mecanismos de control lo suficientemente eficientes para identificar los movimientos de estos grupos en relación a la captación de fondos. Así por ejemplo, tanto los proveedores de servicios de cambio de monedas virtuales por monedas fiduciarias (es decir, las monedas y billetes de designados como medio legal y el dinero electrónico de un país aceptado como medio de cambio en el país expedidor), así como los proveedores de servicios de custodia de monederos electrónicos no están obligados a detectar actividades sospechosas. Esto permite que los grupos terroristas puedan transferir dinero hacia los sistemas financieros de los Estados dentro de las redes de monedas virtuales ocultando transferencias o gozando de cierto grado de anonimato en esas plataformas.

A día de hoy es un reto conocer las nuevas tendencias, especialmente en lo que se refiere a la manera de financiar y ejecutar las operaciones de los grupos terroristas. Sin olvidar que los sistemas tradicionales se siguen utilizando, estos conviven con herramientas más sofisticadas que utilizan tecnologías modernas que están ganando popularidad como sistemas de financiación alternativos o se benefician de exenciones de requisitos jurídicos. Es por ello necesario adoptar nuevas medidas destinadas a garantizar una mayor transparencia de las transacciones financieras, de las sociedades y otras entidades jurídicas, así como de los fideicomisos (del tipo *trust*) con el fin de mejorar el marco preventivo vigente y de luchar más eficazmente contra la financiación del terrorismo. Es importante mencionar que las medidas tomadas deben ser proporcionales a los riesgos de tal manera que el control no suponga una merma en los derechos del resto de la ciudadanía

especialmente en el respeto de los derechos fundamentales como son el derecho a la intimidad o a protección de datos.

En este sentido, instituciones como el Grupo de Acción Financiera Internacional (GAFI) o la Organización de Cooperación y Desarrollo Económicos (OCDE) han conseguido mejoras significativas en la transparencia global del entorno económico en la adopción y aplicación de normas para detectar los sistemas de captación de fondos, tanto en la prevención del blanqueo de capitales como de la financiación del terrorismo. Junto a ellas la información ofrecida por las entidades de crédito y las entidades financieras, así como la información relativa a la idoneidad y honorabilidad de directores y partes interesadas, los mecanismos de control internos, la gobernanza o el cumplimiento y la gestión del riesgo, resultan a menudo indispensables para la supervisión adecuada de la lucha contra el blanqueo de capitales y la financiación del terrorismo de dichas entidades.

Hay por tanto una apuesta por conseguir una colaboración a nivel internacional en la que el papel de la ONU y de la Unión Europea (UE), a través de las agencias de Europol y Eurojust, junto con instituciones como Interpol son fundamentales para conseguir si no frenar al menos disminuir la proliferación de los grupos terroristas protagonistas que operan en cualquier lugar del planeta.

4.1. El papel Naciones Unidas en el control de la financiación de los grupos terroristas

La lucha contra la financiación de grupos terroristas es una preocupación importante a nivel internacional, y las Naciones Unidas (ONU) desempeñan un papel crucial en este esfuerzo proporcionando un marco global para la cooperación y la adopción de medidas concretas para prevenir la financiación de grupos terroristas. Para abordar la cuestión de la financiación del terrorismo esta Organización cuenta con diferentes instrumentos entre los que destacan los siguientes:

4.1.1. Creación de un marco legal internacional

A través de la creación de un marco legal en el seno de la ONU se trabaja para desarrollar y promover la cooperación entre los Estados en la

lucha contra la financiación del terrorismo. Esto se hace especialmente a través de acuerdos internacionales como por ejemplo el Convenio Internacional para la Represión de la Financiación del Terrorismo (1999)³⁴ y de Resoluciones del Consejo de Seguridad que imponen medidas específicas destinadas a prevenir y combatir la financiación del terrorismo. Estas resoluciones pueden incluir sanciones financieras, embargos de activos y restricciones a las transacciones financieras. Entre ellas se encuentran la Resolución 2195 (2014), sobre Amenazas a la paz y a la seguridad, y las Resoluciones 2199 (2015) y 2253 (2015), sobre Amenazas a la paz y a la seguridad internacionales causadas por actos terroristas, del Consejo de Seguridad de las Naciones Unidas³⁵.

4.1.2. Lista de sanciones

La ONU mantiene una lista de individuos y entidades vinculados a grupos terroristas que están sujetos a sanciones financieras. Los Estados miembros están obligados a implementar estas sanciones y tomar medidas para evitar la financiación de estas personas y organizaciones. Para ello Naciones Unidas con la cooperación internacional de los Estados junto con los cuales comparte información sobre actividades financieras sospechosas de presuntos grupos terroristas y coordinar acciones para combatir la financiación del terrorismo. Esto incluye el intercambio de inteligencia y la colaboración entre agencias de seguridad y organismos financieros de diferentes países. La incorporación precisa y oportuna de las revisiones a la lista es fundamental para que los Estados miembros puedan ejecutar las sanciones.

4.1.3. Colaboración con organismos especializados en la lucha contra la financiación de terrorismo

Para llevar a cabo su acción contra los grupos terroristas y en concreto para frenar los mecanismos de financiación, la ONU trabaja junto con el

³⁴ Consultar en https://legal.un.org/avl/intro/welcome_avl.html (consultado el 28 de diciembre de 2023).

³⁵ Consultar las Resoluciones en <https://www.un.org/securitycouncil/es/content/resolutions-adopted-security-council-2014> (consultado el 28 de diciembre de 2023).

Grupo de Acción Financiera (GAFI). Este organismo no es una agencia de la ONU, GAFI es un organismo intergubernamental que trabaja en estrecha colaboración con la ONU y otros organismos internacionales. Su actividad se centra en el desarrollo y la promoción de políticas para combatir el lavado de dinero y la financiación del terrorismo, estableciendo estándares y evaluando la efectividad de los sistemas nacionales en este sentido.

4.2. La función de la Unión Europea en la financiación de los grupos terroristas

La UE se ha convertido en los últimos años en objetivo de grupos terroristas que actúan preferentemente con cédulas locales y «lobos solitarios» creando el terror en los espacios más poblados de las ciudades. Casos como los atentados de Barcelona (2017) o París (2015) son solo algunos ejemplos de como los terroristas buscan notoriedad al mismo tiempo que intentan quebrar el Estado de Derecho que tanto trabajo le ha costado alcanzar a Europa.

Es por ello que desde su vertiente regional la UE aborda la lucha financiación de grupos terroristas mediante una combinación de medidas legislativas, instrumentos de cooperación y supervisión. Aquí hay algunas formas en que la UE actúa en la lucha contra la financiación del terrorismo:

a) Legislación contra el Lavado de Dinero y la Financiación del Terrorismo

La UE ha adoptado una serie de directivas y regulaciones que establecen estándares comunes para prevenir el lavado de dinero y la financiación del terrorismo en los Estados miembros. Estas normativas establecen requisitos para la identificación de clientes, la diligencia debida en las transacciones financieras y la notificación de transacciones sospechosas. Son numerosas las Directivas adoptadas por la UE en esta materia para conseguir una política armonizada entre sus Estados miembro. Actualmente está en vigor la Directiva (UE) 2018/843 del Parlamento Europeo y del Consejo de 30 de mayo de 2018³⁶

³⁶ La Directiva (UE) 2018/843 del Parlamento Europeo y del Consejo de 30 de mayo de 2018 por la que se modifica la Directiva (UE) 2015/849 relativa a la prevención de la utilización del sistema financiero para el blanqueo de capitales o la financiación del terrorismo, y por la que se modifican las Directivas 2009/138/CE y 2013/36/UE, L56 de 9 junio de 2018.

que no solo tiene por objeto detectar e investigar el blanqueo de capitales, sino también prevenirlo³⁷. Asimismo, destacar el acuerdo alcanzado entre el Consejo y el Parlamento Europeo para la creación de una nueva Autoridad de Lucha contra el Blanqueo de Capitales y la Financiación del Terrorismo (ALBC), pieza fundamental del paquete de medidas contra el blanqueo de capitales, cuya misión es proteger a los ciudadanos y el sistema financiero de la Unión Europea contra el blanqueo de capitales y la financiación del terrorismo.

La Directiva ha establecido diferentes mecanismos para combatir los riesgos relacionados con el anonimato en las transacciones a través de las denominadas Unidades de Inteligencia Financiera (UIF) que tienen alcance nacional para obtener informaciones que les permitan asociar las direcciones de las monedas virtuales a la identidad del propietario de la moneda virtual. Así mismo establecen límites a las relaciones de negocios o las transacciones que implican a terceros países de alto riesgo cuando se detecten insuficiencias significativas en el sistema de lucha contra el blanqueo de capitales y la financiación del terrorismo de los terceros países en cuestión, a menos que se apliquen medidas atenuantes o contramedidas suplementarias adecuadas. Esa limitación ha de aplicarse sin menoscabo alguno de las obligaciones de la Unión en materia de comercio internacional, especialmente las disposiciones del Acuerdo General sobre el Comercio de Servicios.

b) Listas de Sanciones y Congelación de Activos

La UE mantiene listas de sanciones que incluyen individuos y entidades vinculados a grupos terroristas. Los Estados miembros están obligados a aplicar medidas como la congelación de activos y restricciones financieras contra aquellos que figuran en estas listas todo ello a través de mecanismos de coordinación a través de los cuales se aborden las amenazas transfronterizas de manera más efectiva. Esto dificulta que los grupos terroristas accedan a fondos y recursos si ninguna limitación y convencidos de su impunidad.

³⁷ Ver en este sentido también la Comunicación de la Comisión al Parlamento Europeo y al Consejo titulada «Plan de acción para intensificar la lucha contra la financiación del terrorismo» COM/2016/050 final

c) Colaboración entre las agencias europeas y las instituciones internacionales

La UE se apoya en una serie de organismos para frenar el avance del terrorismo en Europa. Destacan en este sentido la Agencia Europea de Policía (Europol) que desempeña un papel clave en la lucha contra la financiación del terrorismo en el ámbito de la UE. Para desarrollar su labor facilita la cooperación entre las fuerzas de seguridad de los Estados miembros, realiza análisis financieros y coordina operaciones conjuntas. La Agencia Europea de Supervisión del Sistema Financiero (ESMA) actúa contribuyendo a la supervisión y la implementación de medidas contra el lavado de dinero y la financiación del terrorismo en el sector financiero de la UE. Al mismo tiempo trabaja para garantizar que las instituciones financieras cumplan con los requisitos establecidos por la legislación de la UE. Así mismo se ha reforzado el papel con otros actores a nivel internacional, incluidas las Naciones Unidas y el Grupo de Acción Financiera (GAFI). Esta colaboración busca fortalecer los esfuerzos globales para prevenir y combatir la financiación del terrorismo.

d) Inteligencia Financiera

La UE fomenta la recopilación y el intercambio de inteligencia financiera entre los Estados miembros lo que implica la identificación de patrones financieros sospechosos y la adopción de medidas proactivas para prevenir la financiación del terrorismo.

En conjunto, estas medidas buscan crear un marco integral que aborde la financiación del terrorismo en la UE, promoviendo la cooperación entre los Estados miembros y garantizando la implementación efectiva de las normativas y sanciones establecidas a nivel europeo.

Son fundamentales para el desarrollo de esta función las denominadas Unidades de Inteligencia Financiera (UIF) que desempeñan un importante papel en la detección de las operaciones financieras de las redes terroristas, especialmente transfronterizas, y en la identificación de quienes las respaldan mediante financiación. Estos servicios podrían tener un papel fundamental para descubrir la facilitación de delitos de terrorismo y las redes y sistemas de las organizaciones terroristas, sin embargo, debido a la falta de normas internacionales prescriptivas, las UIF carecen de reglas

uniformes para determinar sus funciones, competencias y potestades. Es por ello que el papel de los Estados miembros es fundamental para garantizar un planteamiento eficaz y coordinado en las investigaciones financieras relacionadas con el terrorismo, incluidas las relacionadas con el uso indebido de monedas virtuales.

En el desempeño de sus funciones, las UIF deben tener acceso a la información y al intercambio de datos a través de la cooperación con los servicios policiales y judiciales. Siempre que se sospeche la existencia de delitos y, con mayor razón, de financiación del terrorismo, la información debe circular directa y rápidamente, sin demoras indebidas.

Ello permitirá que las UIF puedan analizar la información que reciban y establecer vínculos entre transacciones sospechosas y la actividad delictiva subyacente a fin de prevenir y combatir el blanqueo de capitales y la financiación del terrorismo. Su labor es la de comunicar los resultados a las autoridades competentes cuando existan motivos para sospechar de la existencia de blanqueo de capitales o financiación del terrorismo. Sin embargo las UIF han aludido a dificultades en el intercambio de información basadas en las diferencias en las definiciones nacionales de determinados delitos subyacentes, como los delitos fiscales, que no han sido objeto de armonización por el Derecho de la Unión si bien esto no debe ser una excusa para obstaculizar el intercambio de información así como su comunicación a las autoridades competentes tanto de los Estados Miembros como de terceros países en relación con el blanqueo de capitales, los delitos subyacentes conexos y la financiación del terrorismo, todo ello en consonancia con las Recomendaciones del GAFI y los Principios Egmont para el Intercambio de Información entre las Unidades de Inteligencia Financiera.

4.3. El papel de Interpol y Europol para combatir la financiación de los grupos terroristas

Tanto la Interpol (Organización Internacional de Policía Criminal)³⁸ como la Europol (Agencia de Policía de la Unión Europea)³⁹, desempeñan

³⁸ <https://www.interpol.int/es> (consultado el 8 de diciembre de 2024).

³⁹ <https://www.europol.europa.eu/about-europol:es> (consultado el 8 de diciembre de 2024)

un papel fundamental en la cooperación internacional para combatir la financiación de grupos terroristas. Aunque no tienen poderes de arresto y no están autorizadas para actuar de manera autónoma, sirven para facilitar la colaboración entre las fuerzas de seguridad de diferentes países.

El papel que desempeñan en la lucha contra el terrorismo se basa en:

a) El intercambio de Información

Facilitan el intercambio rápido y seguro de información entre las fuerzas de seguridad de los países miembros. Esto incluye datos relacionados con transacciones financieras sospechosas, cuentas bancarias y otras actividades financieras vinculadas a la financiación del terrorismo.

b) Creación de una Base de Datos Global

Interpol mantiene una base de datos global que contiene información sobre individuos y entidades vinculadas al terrorismo, incluyendo aquellas involucradas en la financiación de actividades terroristas. Esta base de datos permite a los países miembros acceder y compartir información de manera efectiva.

c) Emisión de notificaciones y alertas

Emiten notificaciones y alertas a través de su red global para informar a las fuerzas de seguridad sobre amenazas específicas, personas buscadas y actividades financieras sospechosas relacionadas con el terrorismo. Estas notificaciones facilitan una respuesta coordinada y rápida entre los países miembros.

d) Capacitación y Asistencia Técnica

Proporciona capacitación y asistencia técnica a las fuerzas de seguridad de los países miembros para fortalecer sus capacidades en la identificación y la investigación de la financiación del terrorismo. Esto incluye el desarrollo de habilidades en análisis financiero y la aplicación de prácticas efectivas.

e) Análisis Financiero

Realizan análisis financieros para identificar patrones y tendencias en las actividades financieras asociadas con el terrorismo. Esto implica examinar transacciones, seguir flujos de fondos y analizar cuentas bancarias para descubrir conexiones y redes financieras relacionadas con grupos terroristas.

f) Operaciones Conjuntas Colaboración con Otros Organismos Internacionales

Coordinan operaciones conjuntas entre los países miembros para abordar casos específicos de financiación del terrorismo al mismo tiempo que facilita la colaboración directa entre las fuerzas de seguridad, lo que puede llevar a la identificación y desmantelamiento de redes financieras vinculadas a grupos terroristas. Su coordinación con Naciones Unidas y el Grupo de Acción Financiera (GAFI), para garantizar una respuesta integral y coordinada es fundamental para luchar contra la financiación del terrorismo a nivel mundial.

En resumen, estas organizaciones actúan como un facilitador clave en la cooperación internacional entre las fuerzas de seguridad para prevenir y combatir la financiación de grupos terroristas. Su enfoque se centra en el intercambio de información, la emisión de alertas, la capacitación y la coordinación de operaciones conjuntas para abordar las amenazas financieras asociadas al terrorismo.

5. Conclusiones

En consonancia con su naturaleza política y revolucionaria, se puede considerar a día de hoy que las organizaciones terroristas están desarrollando una economía de guerra basada en la realización de atentados que se financian con presupuestos bastante reducidos. Al contrario de lo que pueda parecer esta limitación dificulta enormemente el control de estos grupos por parte de las agencias de seguridad e inteligencia de los Estados.

El anonimato, la transferencia de cuantías pequeñas, el uso de fuentes legales con finalidad ilegal (microfinanciación, tarjetas prepago, *hawalla*, la *dark web*) contribuyen a su invisibilidad convirtiéndolas en tremendamente peligrosas.

Esto convierte a las actividades terroristas en conflictos asimétricos tanto en su aspecto político al enfrentar actores no estatales contra los cuerpos de

seguridad del Estado, como por su configuración económica al utilizar los recursos unos para armarse y los otros para defenderse.

Por otro lado, hay que tener las diferentes finalidades para las que son recaudados los recursos dependiendo de sus fines políticos, o sus necesidades logísticas, la propaganda o la atención social a sus bases. Todo ello se traduce en una gran variedad de formas de financiación con origen legal o ilegal dependiendo de la estructura y las necesidades de la organización terrorista en cada momento.

No obstante, las propias comunidades que los apoyan comienzan a rechazar actuaciones violentas como los secuestros, puede hacer disminuir o incluso desaparecer su utilización ya que el control de sus acciones es fundamental para mantener su capacidad para obtener recursos. En este sentido se ha podido comprobar una estrecha relación entre el nivel de captación de recursos y la capacidad de las organizaciones terroristas para captar militantes armados y desarrollar campañas de atentados, validándose así la idea de que la financiación juega un papel clave en su éxito o en su fracaso. Otro factor importante es el que presentan las entidades asociativas y caritativas en la obtención de recursos de origen legal.

Finalmente sería importante destacar la deriva hacia el mundo virtual en el que se está situando la captación de recursos virando hacia un ciberconflicto que se libra en las redes y en el uso de medios de pago virtuales que complican cada vez más un escenario ya de por sí oscuro y lleno de obstáculos.

Bibliografía

- BEEKARRY, N., «International Anti-Money Laundering and Combating the Financing of Terrorism Regulatory Strategy: A Critical Analysis of Compliance Determinants in International Law», *Northwestern Journal of International Law and Business*, nº 31, 2011, p. 137
- BERGMAN, M., *The Deep Web: surfacing hidden value*, 2001
- BUESA BLANCO, M., «Financiación del terrorismo. Economía del terrorismo», *ICE*, nov-dic, nº 893, 2016, pp. 27-50
- BUESA BLANCO, M., «War and Terrorism: The Predatory War Model», en MIKEL BUESA y THOMAS AUMERT (eds.), *The Economic Repercussions of Terrorism*, Oxford: Oxford University Press, 2010
- FONT, N., «Trust in the European Union in challenging times», *Relaciones internacionales*, 28 (56), 2019, pp. 285-287 (consultado el 17 de enero

- de 2024) http://www.scielo.org.ar/scielo.php?script=sci_arttext&pid=S2314_27662019000100024&lng=es&tlng=es.
- FREEMAN, M., «Sources of Terrorism Financing: Theory and Typology», en MIKEL FREEMAN (ed), *Financing Terrorism: Case Studies*, Surrey: Ashgate e-Book, 2012
- GARCÍA VÁZQUEZ, B., «El derecho internacional frente a los nuevos medios y espacios en que desarrollar la guerra: La ciberguerra», *Revista Chilena de Derecho y Tecnología*, vol.10 nº 2, 2021, pp. 1-27 (consultado el 12 de enero de 2024). <http://grids.ucs.indiana.edu/courses/xinformatics/searchindik/deepwebwhitepaper.pdf>
- JIMÉNEZ CASTILLO, M.C., *Economía del desarrollo humano y microfinanciación: Una aproximación a los determinantes de microcrédito* (Tesis Doctoral Inédita), Universidad de Sevilla, Sevilla, 2013
- LAURENT CHATAIN, P. et al., «Integrity in Mobile Phone Financial Services: Measures for Mitigating the Risks from Money Laundering and Terrorist Financing», *The World Bank*, 2008 <https://doi.org/10.1596/978-0-8213-7556-3>
- PARRA RODRIGUEZ, C., *Empresas con conciencia*, Editorial Viceversa, Barcelona, 2010
- PASSAS, N., y GIMÉNEZ-SALINAS FRAMIS, A., «La financiación del terrorismo de Al Qaeda: mitos y realidades», *Inteligencia y Seguridad. Revista de Análisis y Prospectiva*, nº 2, septiembre 2007, pp. 47-78
- RANSTORP, M., «La financiación del terrorismo: principales actores, estrategias y fuentes», *Afkar Ideas*, primavera 2018, pp. 52-55
- RUDNER, M., «Hizbullah Terrorism Finance: Fund-Raising and Money-Laundering», *Studies in Conflict and Terrorism*, vol. 33, nº 8, 2010, pp. 700-715
- SATOSHI NAKAMOTO, I., «Bitcoin open source implementation of P2P currency», 2009. <http://p2pfoundation.ning.com/forum/topics/bitcoin-open-source> (consultado 10 enero 2024)
- SPALEK, B., «Community Policing, Trust, and Muslim Communities in Relation to “New Terrorism”», *Politics Policy*, vol. 38, issue 4, 2010, pp. 653-886
- TORRES SORIANO, M., «Terrorismo yihadista y nuevos usos de Internet: la distribución de propaganda», Real Instituto Elcano. ARI, nº 110, 2009

- UREÑA CENTENO, F., «Ciberataques, la mayor amenaza actual», *IEES*, nº 9, 2015, pp. 1-18
- VITTORI, J., *Terrorist Financing and Resourcing*, New York, Palgrave Macmillan, 2011
- YUSTE GONZÁLEZ, C., *Deep web y monedas virtuales: entorno privilegiado para las organizaciones terroristas*, Trabajo Fin de Master (inédito), Universidad de la Rioja, 2015

A indissociável relação entre o terrorismo, o branqueamento e o crime organizado

The indissociable relationship between terrorism, money laundering and organized crime

José Daniel Tavares

Resumo: O aumento do terrorismo, a crescente transnacionalidade do crime organizado e do branqueamento das suas vantagens ilícitas utilizado, entre outros fins, como forma de financiamento ao terrorismo, criam ameaças que colocam em causa a segurança das pessoas, das comunidades e dos próprios Estados. A ligação do terrorismo ao crime organizado aumenta esse perigo, fazendo depender a resposta a essas ameaças de uma eficaz cooperação internacional.

Palavras-chave: Cooperação internacional; Financiamento; Repressão; Terrorismo.

Abstract: The rise of terrorism, the growing transnationality of organized crime and the laundering of its illicit advantages used, among other purposes, as a means of financing terrorism, create threats that jeopardize the security of people, communities and States themselves. The connection between the terrorism and the organized crime increases this danger, making the response to these threats depend on effective international cooperation.

Keywords: financing; international cooperation; repression; terrorism.

Sumário: 1. Introdução; 2. Ordem jurídica internacional: Organização das Nações Unidas, Conselho da Europa e União Europeia; 2.1. Organização das Nações Unidas e Conselho da Europa; 2.1.1. Terrorismo; 2.1.2. Crime organizado, branqueamento e financiamento do terrorismo; 2.2. União Europeia; 2.2.1. Terrorismo; 2.2.2. Crime organizado, branqueamento e financiamento do terrorismo; 3. Ordem jurídica nacional: Portugal, os Estados estrangeiros e as Organizações Internacionais como destinatários do terrorismo; 3.1. Terrorismo e seu financiamento; 3.2. Crime organizado e branqueamento; 4. Prevenção e combate ao terrorismo, ao crime organizado e ao branqueamento; 4.1. União Europeia; 4.2. Portugal, medidas especiais de combate: registo de voz e imagem, quebra do sigilo bancário, ações encobertas e proteção de testemunhas; 4.2.1. Terrorismo; 4.2.2. Crime organizado

e branqueamento; 4.2.3. O Tribunal Europeu dos Direitos do Homem e o dever dos advogados de denúncia; 5. Conclusões.

Abreviaturas: AC: Associação Criminosa; AR: Assembleia da República; AT: Associação Terrorista; CO: Crime Organizado; DR: Diário da República; EEMM: Estados Membros; OC: Organização Criminosa; OT: Organização Terrorista; PE: Parlamento Europeu; PR: Presidente da República; RASI: Relatório Anual de Segurança Interna; SIS: Sistema de Segurança Interna; TEDH: Tribunal Europeu dos Direitos do Homem; TUE: Tratado da União Europeia; TFUE: Tratado de Funcionamento da União Europeia.

1. Introdução

A Diretiva (UE) 2017/541 do Parlamento Europeu (PE) e do Conselho relativa à luta contra o terrorismo refere que os atos terroristas se encontram entre as mais gravosas violações dos valores universais fundamentais em que a União se baseia, tais como os relativos à dignidade humana, à liberdade, à igualdade à solidariedade e ao gozo dos direitos humanos e das liberdades¹.

A crescente ligação entre as ameaças à segurança interna e internacional, o terrorismo, o crime organizado (CO) e o branqueamento usado para o financiamento ao terrorismo, fazendo perigar na sombra a segurança dos cidadãos e dos Estados, reclamam atenção de toda a comunidade internacional, conforme decorre dos vários Relatórios Anuais de Segurança Interna (RASI's) elaborados pelo Sistema de Segurança Interna (SIS)² que incluem o terrorismo e o CO entre as preocupações e ameaças à segurança global que se projetam na segurança interna³.

¹ Diretiva (UE) 2017/541 do Parlamento Europeu (PE) e do Conselho, de 15 de março de 2017 (JO L nº 88, de 31 de março de 2017), considerando nº 2. Transposta para a ordem jurídica portuguesa pela Lei nº 16/2019, de 16 de fevereiro, que alterou pela quinta vez a Lei nº 52/2003, de 22 de agosto (Lei de Combate ao Terrorismo).

² Previstos na Lei nº 53/2008, de 29 de agosto (Lei de Segurança Interna).

³ Tais preocupações estão expressas nos referidos relatórios, designadamente: pp. 36-38 do RASI 2012; pp. 28-32, pp. 309 e 343 do RASI 2013; pp. 5-8, p. 125 e p. 179 do RASI 2014; pp. 76-86 do RASI 2015; pp. 71-80 do RASI 2016; pp. 67-76 do RASI 2017; pp. 76-85 do

Encontramos esta ligação entre o crime organizado e os grupos terroristas registada na mesma diretiva⁴, a qual que salienta que «[o] comércio ilícito de armas, petróleo, estupefacientes, (...) o tráfico de seres humanos, a coação e a extorsão tornaram-se formas lucrativas de financiamento dos grupos terroristas»⁵.

Aquela conexão está também presente em alguns diplomas nacionais como é o caso da Lei nº 5/2002, de 11 de Janeiro, relativas à recolha de prova, quebra de segredo profissional e perda de bens a favor do Estado, e na Lei nº 101/2001, de 25 de agosto, regime jurídico das ações encobertas para fins de prevenção e investigação criminal, diplomas que na sua íntegra são aplicáveis, entre outros, aos crimes de associação criminosa e às infrações terroristas, infrações relacionadas com um grupo terrorista, infrações relacionadas com atividades terroristas e financiamento do terrorismo⁶.

O terrorismo constitui, ele próprio, uma forma de crime organizado concentrando em si a generalidade das características⁷ próprias do funcionamento da associação criminosa (AC) ou organização criminosa (OC)⁸, sendo diferentes

RASI 2018; pp. 78-84 do RASI 2019; pp. 98-103 do RASI 2020; p. 9, pp. 29-33, p. 80, e pp. 128-129 do RASI 2021; p. 8, p. 25, p. 28, p. 81, p. 126 e p. 128 do RASI 2022. Disponíveis em URL: www.portugal.gov.pt/download-ficheiros (consulta feita em 29 de julho de 2023).

⁴ Que refere no considerando nº 13 que tais ligações constituem uma ameaça cada vez maior à segurança da União Europeia.

⁵ *Cfr.* também acerca desta ligação, o considerando nº 2 da Decisão-Quadro 2008/841/JAI do Conselho, de 24 de outubro de 2008 (JO L 300, de 11 de novembro de 2008). HELENA CARRAPIÇO, *O Crime Organizado Transnacional na Europa: Origens, Práticas e Consequências*, Lisboa, Instituto de Defesa Nacional, 2006, p. 3, referindo o ataque terrorista de 11 de setembro de 2001 em Nova Iorque, considera que «[p]oucos são aqueles que ousam olhar noutra direção e que se apercebem da existência de outras fontes de insegurança, potencialmente tão perigosas ou mais que o próprio terrorismo», designadamente o branqueamento que lhe serve de fonte de financiamento.

⁶ Ambos os diplomas integram medidas especiais de investigação e inquérito à criminalidade organizada. As conexões referidas estão presentes nas alíneas b) e j) do nº 1 do artigo 1º da Lei nº 5/2002, de 11 de janeiro, e nas alíneas f) e j) do artigo 2º da Lei nº 101/2001, de 25 de agosto. Tais normativos legitimam a aplicação aos referidos crimes das medidas especiais constantes no âmbito de aplicação (também conhecido por catálogo) de ambos os diplomas.

⁷ Como a hierarquia, o acordo de vontades no contributo para o fim criminoso comum, a divisão de tarefas, e a estabilidade temporal.

⁸ Diferentes designações são usadas nos vários instrumentos jurídicos para referir as associações, organizações ou grupos envolvidos no crime organizado: «Grupo Criminoso Organizado» (Convenção de Palermo), «Organização Criminoso» (Decisão-Quadro 841/JAI do Conselho,

os fins essenciais prosseguidos: políticos e/ou religiosos ou híbridos (parte política/religiosa e parte criminosa visando o lucro para garantir o seu financiamento) na associação terrorista (AT) organização terrorista (OT)⁹ e obtenção de elevados lucros através da oferta de bens e serviços ilícitos nas OC's¹⁰.

A gravidade das consequências do terrorismo levou já a um forte debate no sentido de tal crime poder ser considerado como um crime contra a humanidade e incluído na competência do Tribunal Penal Internacional, pretensão que, não obstante, apresenta algumas dificuldades¹¹.

A eficácia do combate ao terrorismo, ao branqueamento e ao crime organizado depende de uma sólida cooperação internacional assente numa real vontade de colaboração por parte dos Estados.

de 24 de outubro de 2008) e, no direito interno, «Grupo», «Organização» ou «Associação» (artigo 299º do Código Penal português e legislação avulsa).

⁹ O artigo 3º da Lei nº 52/2003, de 22 de agosto (Lei de Combate ao Terrorismo) usa as terminologias «grupo, organização ou associação terrorista». Sobre o terrorismo como forma de crime organizado, *cfr.* JOSÉ BRAZ, *Investigação Criminal, a Organização, o Método e a Prova. Os Desafios da Nova Criminalidade*, 5ª ed., Coimbra, Almedina, 2020, pp. 314-318.

¹⁰ São exemplos dessas atividades ilícitas o tráfico humano e de órgãos, de estupefacientes, de armas, de veículos, de objetos de arte furtados, exploração sexual, crimes informáticos, corrupção, fraudes fiscais extorsão/proteção de empresas e negócios *racket*. Existem ligações estratégicas, temporárias e instrumentais entre as OC's e as OT's em função da recíproca utilidade pontual de certas ações, como a garantia de *corredores de passagem* pelas OT's às OC's em zonas de conflito para a circulação, entre outros, de estupefacientes, contrabando e tráfico de pessoas a troco de financiamento, obtenção de armamento e de documentação falsa (PKK (Curdistão), *Sendero Luminoso* (Peru) e as Forças Armadas Revolucionárias da Colômbia-FARC [financiadas por máfias italianas para controlarem os campos com plantas narcóticas]). As FARC assinaram um acordo de paz em 2016 com a Colômbia. Acerca de diversas organizações de «narcoguerrilha», *cfr.* ALAN BAUER E XAVIER RAUFER, *A Globalização do Terrorismo*, Prefácio, Lisboa, 2003, pp. 172-174

¹¹ A competência do Tribunal Penal Internacional relativamente aos crimes contra a humanidade encontra-se prevista na alínea b) do nº 1 do artigo 5º do respetivo Estatuto, assinado em Roma em 17 de julho de 1998. Aprovado para ratificação pela Resolução da Assembleia da República (AR) n.º 3/2002, de 18 de janeiro e ratificado pelo Decreto do Presidente da República (PR) n.º 2/2002, de 18 de janeiro (publicado no Diário da República (DR) I-A, n.º 15, de 18 de janeiro de 2002). Veja-se a propósito de o terrorismo poder ser considerado como um crime contra a humanidade, ANTOINE GARAPON, *Crimes que não se podem punir nem perdoar* (trad. Pedro Henriques) Lisboa: Instituto Piaget, 2004, pp. 127-131; JORGE BACELAR GOUVEIA, *Direito Internacional Penal – Uma Perspectiva Dogmático-Crítica*, Coimbra: Almedina, 2008, pp. 284-288; e JÓNATAS MACHADO, *Direito Internacional. Do Paradigma Clássico ao pós-11 de setembro*, 4ª ed., Coimbra: Coimbra Editora, 2013, pp. 477-478.

2. Ordem Jurídica Internacional: Organização das Nações Unidas, Conselho da Europa e União Europeia

2.1. Organização das Nações Unidas e Conselho da Europa

2.1.1. Terrorismo

A globalização e o vertiginoso progresso científico e técnico nos domínios das comunicações proporcionam rapidez de contactos, de criação e extinção de empresas, de colocação e branqueamento de capitais e da sua utilização no financiamento do terrorismo, reclamando, como se referiu, uma forte cooperação internacional para a sua prevenção e combate¹².

No que se refere ao terrorismo assumem particular importância: i) a Convenção da Internacional para a Repressão de Atentados Terroristas à Bomba¹³; ii) a Convenção Internacional para a Eliminação do Financiamento ao Terrorismo¹⁴, *v.g.* os seus preceitos dedicados à cooperação internacional, artigos 8º a 12º (congelamento de fundos, investigações sobre pessoa suspeita presente num Estado, extradição, sigilo bancário), 16º, 18º (branqueamento) 19º e 24º (transferência de suspeitos, garantias processuais, medidas legislativas de prevenção, comunicações); iii) a Convenção Internacional para a Eliminação de Atos de Terrorismo Nuclear¹⁵; e iv) no seio do Conselho da Europa: a Convenção Europeia para a Repressão do Terrorismo¹⁶, o seu Protocolo de

¹² ANABELA MIRANDA RODRIGUES E JOSÉ LUÍS MOTA, *Para uma Política Criminal Europeia*, Coimbra: Coimbra Editora, 2000, p. 15 referem que «[a] globalização é hoje o novo paradigma da política criminal: frente à internacionalização do crime, urge responder com a internacionalização da política de combate ao crime».

¹³ Assinada em Nova Iorque a 12 de janeiro de 1998. Aprovada pela Resolução da AR n.º 40/2001, e ratificada pelo Decreto PR n.º 31/2001, de 25 de junho de 2001 (publicada no DR I-A n.º 145, de 25 de junho de 2001).

¹⁴ Assinada em Nova Iorque a 9 de dezembro de 1999. Aprovada pela Resolução da AR n.º 51/2002, de 27 de junho de 2002, e ratificada por Decreto do PR n.º 31/2002. (publicada no DR I-A n.º 177, de 2 de agosto de 2002).

¹⁵ Assinada em Nova Iorque a 13 de abril de 2005. Aprovada pela resolução da AR n.º 77/2014, de 27 de junho de 2002 e ratificada por Decreto do PR n.º 64/2014 (publicada no DR I n.º 165, de 8 de agosto de 2014).

¹⁶ Assinada em Estrasburgo a 27 de janeiro de 1977. Aprovada pela Lei n.º 19/81, de 18 de agosto (publicada no DR I n.º 188, de 18 de agosto de 1981).

Alteração¹⁷ e a Convenção do Conselho da Europa para a Prevenção do Terrorismo¹⁸.

2.1.2. Crime Organizado, branqueamento e financiamento do terrorismo

Certamente que em relação ao crime organizado começamos por salientar a Convenção das Nações Unidas contra a Criminalidade Organizada Transnacional (Convenção de Palermo)¹⁹ e os seus Protocolos Adicionais relativos, respetivamente, à Prevenção, Repressão e Punição do Tráfico de Pessoas, em especial de Mulheres e Crianças, ao Tráfico Ilícito de Migrantes por via Terrestre, Marítima e Aérea²⁰ e ao Fabrico e Tráfico Ilícitos de Armas de Fogo, suas Partes Componentes e Munições²¹.

Ligado ao branqueamento internacional²², está o financiamento do terrorismo que é facilitado pela insuficiente regulação do sistema bancário e financeiro, pelas novas tecnologias que proporcionam o encobrimento dos movimentos e seus autores e dificultam a prevenção e repressão, pela

¹⁷ Assinada em Estrasburgo a 15 de maio de 2003. Resolução da AR n.º 133/2015 (publicada no DR I n.º 196, de 7 de outubro de 2015).

¹⁸ Assinada em Varsóvia a 16 de maio de 2005. Resolução da AR n.º 101/2015, e ratificada pelo Decreto do PR n.º 74/2015 (publicada no DR I, n.º 142, de 23 de julho de 2015). Acerca do crescendo de obrigações internacionais de criminalização do terrorismo após os atentados de 11 de Setembro de 2001 nos Estados Unidos da América que levaram a que o terrorismo tenha deixado de «ser tratado como um problema meramente interno para passar a ser tratado como uma verdadeira ameaça para a paz e segurança internacionais», cfr. ANTÓNIO MANUEL ABRANTES, «As obrigações internacionais de criminalização impostas pelo Conselho de Segurança das Nações Unidas no âmbito do combate ao Terrorismo», in *Homenagem ao Professor Doutor Germano Marques da Silva*, José Lobo Moutinho *et al.* (coordenadores), vol. I, Lisboa: Universidade Católica Editora, p. 259.

¹⁹ De 15 de novembro de 2000. Aprovada pela Resolução da AR n.º 32/2004, de 2 de abril, ratificada pelo Decreto do PR n.º 19/2004, de 2 de abril (publicada no DR I-A, n.º 79, de 2 de abril de 2004).

²⁰ Ambos de 15 de novembro de 2000. Foram aprovados, ratificados e publicados conjuntamente com a Convenção de Palermo.

²¹ De 31 de maio de 2001. Aprovado pela Resolução da AR n.º 104/2011 e ratificado pelo Decreto do PR n.º 49/2011, de 5 de junho (publicado no DR I, n.º 88, de 6 de maio de 2011).

²² O branqueamento das vantagens obtidas pelas OC's, consiste no afastamento do dinheiro ou dos bens da sua origem ilícita, conferindo-lhe aparência de licitude (ex.: investimento no controlo de empresas e atividades legais, *v.g.* construção civil, turismo, retalho e instalações portuárias).

utilização de profissionais da finança, pelo conhecimento dos locais propícios aos investimentos e pelo facilitismo na criação e extinção de empresas fictícias²³.

Com vista a prevenir a contribuição do branqueamento e do crime organizado para o terrorismo, a própria Convenção de Palermo dedica ao combate e punição do branqueamento os seus artigos 6º e 7º, cumprindo também referir a Convenção das Nações Unidas contra o Tráfico Ilícito de Estupefacientes e de Substâncias Psicotrópicas (Convenção de Viena)²⁴, a Convenção do Conselho da Europa relativa ao Branqueamento, Detecção, Apreensão e Perda dos Produtos do Crime e ao Financiamento do Terrorismo²⁵ que dedica à cooperação internacional grande parte dos seus preceitos²⁶, *v. g.* sobre a perda de instrumentos, bens e produtos do crime, investigação, informações sobre contas e operações bancárias, cooperação entre as unidades de informação financeira e adiamento de transações suspeitas.

Cabe também registar a Convenção do Conselho da Europa sobre a Manipulação de Competições Desportivas que refere o branqueamento das vantagens ilícitas²⁷, assinalando-se ainda a importância do GAFI-Grupo de

²³ O aproveitamento das novas tecnologias e da globalização pelas associações criminosas é referido no Plano de Ação contra a Criminalidade Organizada de 28 de abril de 1997 do Conselho (JO C 251, 15 de agosto de) ao referir que o crime organizado se mostra «perfeitamente capaz de fazer reverter a seu favor a rapidez e o anonimato oferecidos pelas formas de comunicação modernas». Sobre a relação das novas tecnologias com o crime organizado, *cf.*: JOSÉ BRAZ, *Investigação Criminal, a Organização, o Método e a Prova. Os Desafios da Nova Criminalidade*, *cit.*, pp. 299-303 e 308.

²⁴ De 19 de dezembro de 1988. Resolução da AR n.º 29/91, de 9 de junho. Ratificada pelo Decreto do PR n.º 45/91, de 9 de junho (DR I-A n.º 205, de 6 de setembro de 1991). Acerca da perda de bens e do branqueamento, ver a alínea l) do artigo 1º, as subalíneas i) e ii) da alínea b) do artigo 3º, a subalínea i) da alínea c) do artigo 3º, a alínea a) do n.º 1 do artigo 5º e os números 5 e 6 do artigo 5º.

²⁵ De 16 de maio de 2005, em Varsóvia. Resolução da AR n.º 82/2009, de 7 de março. Ratificada por Decreto do PR n.º 78/2009, de 27 de agosto (publicada DR I-A n.º 166, de 27 de agosto de 2009). Esta convenção sucede a outra com a mesma designação, assinada a 8 de novembro de 1990 (publicada no DR I-A n.º 287, de 13 de dezembro de 1997) que considerou o combate ao branqueamento e à criminalidade organizada «cada vez mais um problema internacional».

²⁶ Concretamente trinta e quatro dos seus cinquenta e cinco artigos.

²⁷ De 18 de setembro de 2014. Aprovada pela Resolução da AR n.º 109/2015. Ratificada pelo Decreto do PR n.º 92/2015 (publicada no DR I n.º 53, de 7 de agosto de 2015). O

Ação Financeira Internacional, criado em 1989 pelos 7 países mais industrializados do mundo (G7), visando a atuação concertada e articulada na prevenção e combate ao branqueamento de capitais²⁸.

Ainda neste âmbito cabe referir a importância da Interpol (Organização Internacional de Cooperação Policial), criada em 1956, e que, apesar da sua vocação global, não surgiu originariamente no âmbito da ONU, sendo por esta reconhecida em 1971²⁹.

2.2. União Europeia

2.2.1. Terrorismo

No âmbito da União Europeia, entre outros atos legislativos cabe salientar: i) o Regulamento (CE) n° 2580/2001 do Conselho, relativo a medidas restritivas específicas de combate ao terrorismo³⁰; ii) a Decisão-Quadro do Conselho 2002/475/JAI que recomenda a cooperação entre os Estados Membros (EEMM) na luta contra o terrorismo³¹; iii) a Decisão 2005/671/JAI do Conselho relativa à troca de informações e à cooperação em matéria de infrações terroristas³²; iv) a Decisão 2008/615/JAI do Conselho relativa ao aprofundamento da cooperação transfronteiriça, em particular no domínio da luta contra o terrorismo e a criminalidade transfronteiriça³³, alargando a todos os EEMM os objetivos do Tratado de Prüm de 27 de Maio de 2005³⁴; v) a Decisão-Quadro

artigo 16º aborda o branqueamento dos produtos de infrações penais relativas à manipulação de competições desportivas.

²⁸ Funciona a nível intergovernamental. Composição inicial do G7: Estados Unidos da América, Japão, República Federal da Alemanha, França, Reino Unido, Itália e Canadá. Integra atualmente mais de trinta países. Portugal integra o GAFI desde 1990.

²⁹ Foi antecedida pela Comissão Internacional de Polícia Criminal. Tem sede em Lyon contando com mais de cento e oitenta Estados-membros.

³⁰ De 27 de junho de 2001 (JO L 344, de 28 de dezembro de 2001).

³¹ De 13 de junho de 2002 (JO L 164 de 22 de junho de 2002). Revogada pela Diretiva (UE) 2017/541 do PE e do Conselho, que determina a criminalização de participação nas OT's e a proteção às vítimas. Foi transposta pela Lei n° 52/2003, de 22 de agosto (Lei de Combate ao Terrorismo).

³² De 20 de setembro de 2005 (JO L 253, de 29 de setembro de 2005). Alterada pela Diretiva (UE) 2017/541 do PE e do Conselho.

³³ De 23 de junho de 2008 (JO L 210, de 6 de agosto de 2008).

2008/919/JAI, do Conselho³⁵; vi) a estratégia revista da U. E. no combate à radicalização e ao recrutamento para o terrorismo de 19 de maio de 2014; vii) o Regulamento (UE) n° 656/2014 do PE e do Conselho³⁶ que estabelece regras para a vigilância das fronteiras marítimas externas coordenada pela Agência Europeia de Gestão da Cooperação Operacional nas Fronteiras Externas dos Estados-Membros da União Europeia criada pelo Regulamento n° 2007/2004 do Conselho³⁷; e viii) a Diretiva (UE) 2016/681 do PE e do Conselho relativa à utilização (pelas companhias aéreas) dos dados de identificação dos passageiros (PNR) para prevenção, deteção, investigação e repressão das infrações terroristas e da criminalidade grave³⁸.

Prosseguindo, a já referida Diretiva (UE) 2017/541 do PE e do Conselho relativa à luta contra o terrorismo enumera exaustivamente no seu artigo 3º uma série de crimes graves e condições em que as ofensas contra a vida humana podem constituir infrações terroristas *v.g.* quando cometidos com o objetivo de intimidar gravemente uma população, compelir de forma indevida os poderes públicos ou uma organização internacional à prática ou à abstenção de praticar um ato, desestabilizar ou destruir as estruturas políticas, constitucionais, económicas ou sociais fundamentais de um país ou de uma organização internacional³⁹.

³⁴Celebrado entre a Bélgica, Alemanha, Espanha, França, Luxemburgo, Países Baixos e Áustria, relativo ao aprofundamento da cooperação transfronteiriça, em particular no domínio da luta contra o terrorismo, a criminalidade transfronteiriça e a migração ilegal (a estratégia antiterrorista da União Europeia de 30 de novembro de 2005). *Cf.* URL: register.consilium.europa.eu/doc/srv?l=PT&f=ST%2014469%202005%20REV%204 (consulta feita em 29 de julho de 2023).

³⁵ De 28 de novembro de 2008 (JO L 330 de 2008.12.09). Revogada pela Diretiva (UE) 2017/541 do PE e do Conselho.

³⁶ De 15 de maio de 2014 (JO L 189, de 27 de junho de 2014).

³⁷ De 26 de outubro de 2004 (JO L 349, de 25 de novembro de 2004). Alterado pelo Regulamento (UE) n° 656/2014 do Parlamento Europeu e do Conselho. Visa garantir um controlo (da responsabilidade dos EEMM) uniforme nas fronteiras da União Europeia, com vista a garantir a segurança no mar e criar regras sobre deteção e interceção no mar territorial e no alto mar, na zona contígua, e sobre situações de busca e salvamento e desembarque (artigos 3º a 7º).

³⁸ De 27 de abril de 2016 (JO L 119, 4 de maio de 2016).

³⁹ A Diretiva refere ainda outras atividades relacionadas com o terrorismo, como o incitamento, recrutamento, treino, direção, financiamento, deslocações para fins terroristas e a assistência e proteção às vítimas de terrorismo.

2.2.2 Crime organizado, branqueamento e financiamento do terrorismo

No que concerne ao crime organizado, começamos por referir que a Comunidade Europeia aderiu à Convenção de Palermo⁴⁰ e aos seus Protocolos Adicionais acima identificados⁴¹.

Prosseguindo, registamos entre muitos outros o já referido Plano de Ação contra a Criminalidade Organizada⁴², a Resolução do Conselho sobre a Prevenção e Combate global à Criminalidade Organizada⁴³, a Ação Comum relativa à Participação numa Organização Criminal⁴⁴, a Decisão-Quadro 2008/841/JAI do Conselho que promove a aproximação penal dos EEMM da União Europeia, define OC, obriga os EEMM a adotar medidas penais relativamente a crimes praticados no seio das OC's⁴⁵ e a Resolução do PE sobre a criminalidade organizada na União Europeia⁴⁶.

Relativamente ao branqueamento e financiamento do terrorismo começamos por referir o disposto no artigo 75º do Tratado de Funcionamento da União Europeia (TFUE) incluído nas disposições relativas ao Espaço de Liberdade, Segurança e Justiça, que permite a adoção de regulamentos contendo medidas relativas aos movimentos de capitais e aos pagamentos, como o congelamento de fundos, ativos financeiros⁴⁷.

Prosseguindo, cabe referir: i) a Diretiva do Conselho (91/308/CEE)⁴⁸, alterada pela Diretiva 2001/97/CE do PE e do Conselho⁴⁹, e pela Diretiva

⁴⁰ Decisão do Conselho nº 2004/579/CE (JO L 261, 6 de agosto de 2004).

⁴¹ Respetivamente, as Decisões do Conselho nº 2006/616/CE e nº 2006/617/CE, 2006/618/CE, ambas de 24 de julho de 2006 (JO L 262, de 12 de setembro de 2006) e nº 2014/164/EU, de 11 de fevereiro de 2014 (JO L 89, de 25 de março de 2014).

⁴² De 28 de abril de 1997 (JO C 251, de 15 de agosto de 1997).

⁴³ De 21 de dezembro de 1998 (JO C 408, de 29 de dezembro de 1998).

⁴⁴ De 21 de dezembro de 1998 (JO L 351, de 29 de dezembro de 1998).

⁴⁵ De 24 de outubro de 2008 (JO L 300, de 11 de novembro de 2008); revoga a Ação Comum 98/733/JAI.

⁴⁶ De 25 de outubro de 2011 (JO C 131, de 8 de maio de 2013).

⁴⁷ Acerca das diversas interpretações dadas à articulação entre os artigos 75º e 215º do TFUE, *cf.*: PATRÍCIA FRAGOSO MARTINS, “A Luta Contra o Terrorismo no Entrecruzamento das Dimensões Externa e Interna da Política Europeia de Segurança”, in *Estudos em Homenagem ao Professor Doutor Wladimir Brito*, Mário Ferreira Monte, Joaquim Freitas da Rocha e Maria de Assunção do Vale Pereira (coordenadores), Coimbra: Almedina, 2020, pp. 1267-1280.

⁴⁸ De 10 de junho de 1991 (JO L 116, de 28 de junho de 1991).

2005/60/CE do PE e do Conselho⁵⁰, relativa à prevenção da utilização do sistema financeiro para efeito de branqueamento de capitais e de financiamento do terrorismo, revogada pela Diretiva 2015/849/UE do PE e do Conselho relativa à prevenção da utilização do sistema financeiro para branqueamento ou financiamento do terrorismo⁵¹ que mantém e reforça a necessidade de prevenção do branqueamento; ii) a Decisão-Quadro 2005/212/JAI do Conselho relativa à perda de produtos, instrumentos e bens relacionados com o crime⁵²; iii) a Diretiva 2014/42/UE do PE e do Conselho sobre o congelamento e a perda dos instrumentos e produtos do crime na União Europeia⁵³; iv) a Diretiva 2016/2258/UE do Conselho, respeitante ao acesso às informações contra o branqueamento de capitais pelas autoridades fiscais⁵⁴; v) a Diretiva (UE) 2018/843 do PE e do Conselho relativa à prevenção da utilização do sistema financeiro para efeitos de branqueamento de capitais ou de financiamento do terrorismo⁵⁵; vi) o Regulamento (UE) 2018/1672 do PE e do Conselho relativo ao controlo de valores em dinheiro superiores a € 10 000,00 que entram ou saem da União⁵⁶; e vii) a Diretiva (UE) 2018/1673 do PE e do Conselho relativa ao combate ao branqueamento de capitais através do direito penal⁵⁷.

⁴⁹ De 4 de dezembro de 2001 (JO L nº 344, 28 de dezembro de 2001). Alarga o conceito de branqueamento, estende as obrigações de colaboração a entidades não financeiras e às profissões liberais e afirma que «[a] repressão da criminalidade organizada, em particular, está estreitamente relacionada com a luta contra o branqueamento de capitais».

⁵⁰ De 26 de outubro de 2005 (JO L 309, de 25 de novembro de 2005). A diretiva inicial, 91/308/CEE, estava circunscrita essencialmente às infrações associadas ao tráfico de estupefacientes, tendo sido revogada pela Diretiva 2015/849/UE, do PE e do Conselho.

⁵¹ De 20 de maio de 2015 (JO L 141, de 5 de junho de 2015), que também revoga a Diretiva 2006/70/CE da Comissão, de 1 de agosto de 2006 (JO L 214, de 4 de agosto de 2006).

⁵² De 24 de fevereiro de 2005 (JO L 68, de 15 de março de 2005).

⁵³ De 3 de abril de 2014 (JO L 127, de 29 de abril de 2014).

⁵⁴ De 6 de dezembro de 2016 (JO L 342, de 16 de dezembro de 2016).

⁵⁵ De 30 de maio de 2018 (JO L 156, de 19 de junho de 2018). Transposta pela Lei nº 58/2020, de 31 de agosto. Altera as Diretivas 2009/138/CE e 2013/36/UE e a Diretiva (UE) 2015/849 do PE e do Conselho, de 20 de maio de 2015.

⁵⁶ De 23 de outubro de 2018 (JO L 284, de 11 de dezembro de 2011).

⁵⁷ De 23 de outubro de 2018 (JO L 284, de 12 de novembro de 2018). Também transposta pela Lei nº 58/2020, de 31 de agosto.

3. Ordem jurídica nacional: Portugal, os Estados estrangeiros e as Organizações Internacionais como destinatários do terrorismo

3.1. Terrorismo e seu financiamento

Começamos por registar que a alínea i) do artigo 1º do Código de Processo Penal considera como terrorismo «as condutas que integram os crimes de organizações terroristas, terrorismo, terrorismo internacional e financiamento do terrorismo».

O regime de combate ao terrorismo consta da Lei nº 52/2003, de 22 de agosto⁵⁸, que pune o crime autónomo do OT ou AT exigindo para a sua constituição apenas duas pessoas⁵⁹, a prática das infrações terroristas cujas condutas individuais estão previstas nos números 2 e 3 do artigo 3º e artigo 4º⁶⁰ e ainda o seu financiamento.

Assim, entre outras, são infrações terroristas os atos dolosos abaixo indicados, na medida em que estejam previstos como crime que, pela sua natureza ou pelo contexto em que são cometidos, possam afetar gravemente o Estado, um Estado Estrangeiro ou uma Organização Internacional⁶¹, quando forem praticados com o objetivo de intimidar gravemente certas pessoas, grupos de pessoas ou a população em geral, designadamente ofensas

⁵⁸ Sofreu várias alterações, a última das quais pela Lei nº 02/2023, de 16 de janeiro, que transpõe para a ordem jurídica portuguesa a Diretiva (UE) 2017/541 do PE e do Conselho, de 19 de abril de 2017.

⁵⁹ Contrariamente a outros regimes de crime organizado que exigem o número mínimo de três pessoas, conforme será referido. Conceito de grupo terrorista e de infração terrorista: número 1 do artigo 2º da Lei nº 52/2003 considera grupo terrorista a «associação de duas ou mais pessoas (...) que se mantém ao longo do tempo e atua de forma concertada com o objetivo de cometer infrações terroristas». Penas: i) prisão entre 8 e 15 anos para as condutas de promoção, fundação, adesão e apoio, de acordo com as alíneas a) e b) do nº 1 do artigo 3º; e ii) prisão de 15 a 20 anos para a chefia ou direção de tais organizações (nº 2 do artigo). Diferentemente dos demais regimes punitivos da associação criminosa, é prevista a punição da prática de atos preparatórios da constituição de grupo terrorista (com pena de 1 a 8 anos, nos termos do nº 3 do artigo 3º), admitindo-se também a possibilidade de atenuação ou isenção de pena (nº 4 do artigo 3º).

⁶⁰ As quais são punidas em concurso com o crime de organização terrorista.

⁶¹ O artigo 5º (Terrorismo Internacional) foi revogado, por este âmbito passar a constar do nº 3 do artigo 2º.

à vida, à integridade física, coação, sequestro, tomada de reféns, destruição de instalações governamentais ou públicas, dos sistemas de transporte, de infraestruturas, de locais públicos ou privados, suscetíveis de pôr em perigo vidas humanas ou de causar prejuízos económicos elevados, a captura de aeronaves, de navios ou outros meios de transporte, o fabrico, a posse, a aquisição, o transporte, o fornecimento ou a utilização de explosivos, armas ou munições, incluindo armas químicas, biológicas⁶².

O crime de financiamento do terrorismo encontra-se no artigo 5º-A⁶³, prevendo-se no artigo 6º a responsabilidade criminal das pessoas coletivas.

Adaptando para a interpretação do preceito que criminaliza a OT o que, a propósito do regime geral da OC é doutrinariamente referido sobre o artigo 299º do Código Penal, consideraremos, de acordo com Paulo Pinto de Albuquerque, como promotor ou fundador da OT aquele que tem a ideia, e chefe ou dirigente aquele que «dirige a estrutura de comando e controla o processo de formação da vontade coletiva» e que, em último grau, decide sobre a disponibilidade dos membros⁶⁴.

⁶² Números 3 e 4 do artigo 2º. O nº 1 do artigo 4º pune com pena de 1 a 12 anos de prisão a prática destas infrações terroristas. O mesmo artigo prevê outras infrações terroristas e infrações relacionadas com atividades terroristas como o furto qualificado, roubo, extorsão, burla informática e nas comunicações, abuso de cartão de garantia ou de cartão, dispositivo ou dados de pagamento, falsificação ou contrafação de documento, falsidade informática, contrafação de cartões ou outros dispositivos de pagamento, uso de cartões ou outros dispositivos de pagamento contrafeitos, aquisição de cartões ou outros dispositivos de pagamento contrafeitos ou atos preparatórios da contrafação com vista à prática de uma infração terrorista (nº2), recrutamento (nº6), treino (nº 7), publicitação (nº 8), viagem para treino (nº 10), e para adesão a organização terrorista (nºs 11 e 12). O nº 15 contempla a possibilidade de atenuação ou isenção de pena.

⁶³ Pune com pena de prisão de 8 a 15 anos o fornecimento, recolha ou detenção de fundos ou bens e produtos ou direitos suscetíveis de ser transformados em fundos, com a intenção de utilização ou possibilidade de serem utilizados no planeamento e na preparação ou prática de atos terroristas. O nº 2 prevê condições que não afastam a infração terrorista, o nº 3 a possibilidade de atenuação ou dispensa de pena e o nº 4 clarifica o que se entende por fundos destinados a financiar o terrorismo.

⁶⁴ PAULO PINTO DE ALBUQUERQUE, *Comentário do Código Penal à luz da Constituição da República e da Convenção Europeia dos Direitos do Homem*, 4ª ed., Universidade Católica Editora, Lisboa, 2021, p. 1114. Sobre a caracterização dessas figuras, *cf.* também JORGE FIGUEIREDO DIAS, “Comentário ao artigo 299º”, in *Comentário Conimbricense do Código Penal*, Jorge Figueiredo Dias (direção), Coimbra: Coimbra Editora, 1999, pp. 1155 a 1174 (§ 26 a 33).

Prosseguindo, considera-se membro aquele que, integrando a OT, está disponível para, de acordo com a vontade do grupo, participar nas tarefas que lhe forem atribuídas, podendo não conhecer todos os membros do grupo e/ou não participar em todas as atividades⁶⁵, apoiante aquele que presta auxílio sabendo que tal se destina à OT⁶⁶ e instigador aquele angariador que determina outros à adesão, considerando-se que o bem jurídico protegido é a «paz pública»⁶⁷, relativamente a todos que «o dolo tem por objeto a aquiescência à finalidade comum»⁶⁸.

3.2. Crime organizado e branqueamento

Portugal está internacionalmente comprometido com a criação de mecanismos de prevenção, de investigação, de combate e punição do crime organizado e do branqueamento, não só por ser parte da Convenção de Palermo e dos respetivos Protocolos Adicionais, mas também pelas obrigações que lhe advêm do facto de integrar o processo de construção europeia, designadamente o dever de obediência aos atos legislativos provenientes das Instituições da União.

Deste modo, cumprindo o disposto no artigo 5º da Convenção de Palermo, o direito português consagra no artigo 299º do Código Penal o regime geral de punição do impulso, promoção, fundação, integração, apoio, auxílio⁶⁹, a chefia e direção⁷⁰ das OC's para a prática de um ou mais crimes, caracterizando a OC quanto ao número mínimo de elementos (três), a sua

⁶⁵ O que se torna importante para não ser ilibado da acusação de participação em OT, ainda que alegue que desconhecia certas atividades ou mesmo os restantes membros.

⁶⁶ Designadamente, cedendo um local para depósito de material ou para a efetivação de encontros.

⁶⁷ PAULO PINTO DE ALBUQUERQUE, “O crime de Organização Criminosa no Código Penal Português”, in *Crime Organizado, Análise da Lei 12.850/2013*, Kai Ambos e Eneas Romero (Coordenadores), São Paulo: Marcial Pons, CEDPAL, 2017, p. 280. O autor pronuncia-se também, pp. 280-282, acerca das figuras de membro, apoiante e instigador.

⁶⁸ MANUEL MAIA GONÇALVES, *Código Penal Português Anotado e Comentado*, 16ª ed., Almedina, Coimbra, 2004, p. 908.

⁶⁹ Nomeadamente fornecendo armas, munições, instrumentos de crime, guarda ou locais para as reuniões, ou qualquer auxílio para que se recrutem novos elementos. *Cfr.* n.ºs 1 e 2: com pena de prisão de 1 a 5 anos.

⁷⁰ Número 3: com pena de 2 a 8 anos de prisão. O n.º 4 refere circunstâncias atenuantes.

estabilidade temporal⁷¹ e atuação concertada⁷², sendo fontes do preceito o artigo 263º (associação de malfeitores) do Código Penal de 1886⁷³ no qual se encontram já muitas das características do regime atual e o § 129º *Bildung krimineller Vereinigungen* do *StGB* alemão⁷⁴.

Decorre do artigo 299º do Código Penal que a prática do crime de OC depende apenas de que o grupo se constitua para o cometimento de delitos criminais, não se subordinando a sua aplicação ou definição ao tipo de crimes praticados, a molduras penais mínimas e à obtenção de benefício económico, contrariamente ao que expressam as alíneas a) e b) do artigo 2º da Convenção de Palermo que refere que os crimes praticados tenham a pena mínima de 4 anos e a obtenção daquele benefício e o número 1 do artigo 1º da supra referida Decisão-Quadro nº 2008/841/JAI, o que permite, por exemplo, que possa ser imputado o crime de associação criminosa a um grupo que se destine, por exemplo, à prática de ofensas corporais ou ao homicídio de pessoas por motivos raciais.

Neste sentido se pronuncia o Relatório da Comissão ao PE e ao Conselho de 2016⁷⁵, com base no artigo 10.º da mesma Decisão-Quadro 2008/841/JAI, salientando que, não fazendo referência ao «critério do benefício nem ao

⁷¹ Número 5, que implica que a associação seja durável e não se esgote com a prática de um único crime.

⁷² Número 5: traduz-se no sentimento comum de ligação dos seus membros à AC contribuindo, com a sua ação ou omissão, para o objetivo criminal comum; esse encontro de vontades transforma a AC numa unidade autónoma, diferente e superior às vontades e interesses dos seus membros.

⁷³ Era a seguinte a redação do artigo: «[a]queles que fizerem parte de qualquer associação formada para cometer crimes, e cuja organização ou existência se manifeste por convenção ou por quaisquer outros factos, serão condenados à pena de prisão maior de dois a oito anos, ou, em alternativa, à pena de degredo temporário, salvo se forem autores da associação ou nela exercerem direção ou comando, aos quais será aplicada a pena de dois a oito anos de prisão maior celular, ou, em alternativa, a de prisão maior temporária. § único – Serão punidos como cúmplices os que a estas associações ou quaisquer divisões delas fornecerem ciente e voluntariamente armas, munições, instrumentos do crime, guarida ou lugar para reunião». Mandado publicar por Decreto de 16 de setembro de 1886 (Diário do Governo, de 20 de setembro de 1886. Disponível em URL://www.fd.unl.pt/Anexos/Investigacao/1274.pdf (consulta feita em 17 de maio de 2023).

⁷⁴ Conforme afirma PINTO de ALBUQUERQUE, *O crime de Organização Criminosa no Código Penal Português*, cit., p. 276.

⁷⁵ De 7 de julho de 2016, COM (2016) 448 final.

nível das infrações (moldura penal)» Portugal e outros EEMM alargam «o âmbito de aplicação às organizações criminosas não necessariamente motivadas pela obtenção de lucro e a todos os tipos de infrações penais».

Salientamos ainda que pode ocorrer punição por OC mesmo que o crime a praticar não tenha sido consumado, porque se trata de «intervir num estágio prévio» quando a segurança ainda não foi perturbada mas existe já «um especial perigo de perturbação porque a mera existência de associações criminosas (...) põe em causa o sentimento de paz que a ordem pública visa criar nos seus destinatários»⁷⁶ sendo o crime de OC punido em concurso real com os crimes individualmente praticados no âmbito da organização⁷⁷.

Paralelamente, existem regimes especiais de punição da OC, designadamente para a prática de crimes como o tráfico ilícito de estupefacientes e de substâncias psicotrópicas constante dos números 1 a 3 do artigo 28º do Decreto-Lei nº 15/93, de 22 de Janeiro que, conforme exigido pela Convenção de Viena de 1988 Contra o Tráfico de Estupefacientes⁷⁸, contém requisitos e penas mais gravosos que as do regime geral, punindo a promoção, fundação ou financiamento com pena de 10 a 25 anos de prisão⁷⁹, a colaboração, a adesão ou o apoio com pena de prisão de 5 a 15 anos⁸⁰ e a chefia ou direção com pena de 12 a 25 anos⁸¹, sendo de 2 pessoas o número mínimo de participantes para ocorrer a punição por AC⁸².

⁷⁶ JORGE FIGUEIREDO DIAS, “Comentário ao artigo 299º”, cit., p. 1157. *Cfr.* neste sentido o Acórdão do Tribunal de Relação de Évora, processo nº 24/10.0TELSB.E1, de 2012.12.20, no qual se lê que é o «originar desta realidade autónoma (inexistente na mera participação criminosas) que, pela sua mera existência, representa uma ameaça de tal gravidade que leva o legislador a reprimi-la enquanto tal», acessível em URL://www.dgsi.pt/jtre.nsf/134973db04f39bf2802579bf005f080b/9d42f6ec3b7ed1e380257de10056fa1e?OpenDocument&Highlight=0 (consulta feita em 27 de julho de 2023).

⁷⁷ *Cfr.* acórdão do Tribunal da Relação de Coimbra, processo nº 274/10.9JALRA-B.C1, de 2013.11.27, acessível em URL://www.dgsi.pt/jtrc.nsf/8fe0e606d8f56b22802576c0005637dc/4d499d6f6a75c5e380257c3800385481?OpenDocument (consulta feita em 2023.07.27). Trata-se da concorrência entre o crime «de» organização (de OC) e os crimes «da» organização, isto é, os crimes praticados no seio da mesma organização.

⁷⁸ *Supra* identificada.

⁷⁹ Número 1 do artigo 28º, com pena de prisão de 1 a 5 anos, no regime geral do artigo 299º do Código Penal.

⁸⁰ Número 2 do artigo 28º, com pena de prisão de 1 a 5 anos, no regime geral

⁸¹ Nº 3 do artigo 28º. A correspondente pena no regime geral é de 2 a 8 anos de prisão.

⁸² Número 1 do artigo 28º, sendo de três o número mínimo no regime geral.

Também a OC para branqueamento das vantagens provenientes do narcotráfico tem regime penal agravado face ao regime geral⁸³, punição que tem lugar em concurso efetivo com o crime de branqueamento previsto e punido no artigo 368º-A do Código Penal⁸⁴.

São também objeto de regime especial de punição as associações criminosas para a prática dos crimes contra a verdade desportiva⁸⁵, para o cometimento de crimes tributários⁸⁶, para o auxílio à imigração ilegal⁸⁷, para a prática dos crimes de tráfico e administração de substâncias proibidas no desporto (dopagem)⁸⁸, para o contrabando de produtos relacionados com a defesa⁸⁹ e a organização terrorista prevista e punida pela Lei nº 52/2003, de 22 de agosto já anteriormente caracterizada.

⁸³ Pena de prisão de 2 a 10 anos para quem promover, fundar, financiar ou chefiar tal associação, conforme consta da alínea a) do número 3 do artigo 28º e pena de prisão de 1 a 8 anos para quem colaborar, aderir ou apoiar, como refere a alínea b) do número 4 do artigo 28º.

⁸⁴ Neste sentido, PAULO PINTO DE ALBUQUERQUE, *Comentário do Código Penal à luz da Constituição da República e da Convenção Europeia dos Direitos do Homem*, cit., p. 1116. A associação criminosa para branqueamento das vantagens provenientes de quaisquer outros ilícitos é punida pelo artigo 299º do Código Penal. Em momento posterior serão referidas medidas especiais de prevenção ao branqueamento.

⁸⁵ Artigo 11º da Lei nº 50/2007, de 31 de agosto. Exige o mínimo de três pessoas, sendo as penas de prisão iguais às do regime geral.

⁸⁶ Artigo 89º da Lei nº 15/2001, de 05 de junho. As penas do promotor, fundador e apoiante são iguais entre si e ao regime geral (números 1 e 2): de 1 a 5 anos de prisão; a pena do participante é equiparada à da chefia e direção (número 3): de 2 a 8 anos de prisão, «se pena mais grave não lhe couber, nos termos de outra lei penal». Não refere o número mínimo de participantes, aplicando-se o regime geral de três pessoas.

⁸⁷ Artigo 184º da Lei nº 23/2007, de 4 de julho. Pena superior ao artigo 299 CP para a promoção, fundação, apoio, integração ou auxílio ao recrutamento (números 1 e 2): pena de prisão de 1 a 6 anos. Para a chefia ou direção (número 3): pena de prisão de 2 a 8 anos (igual ao regime geral). É prevista a punição da tentativa (número 4), contrariamente ao regime geral do artigo 299º do Código Penal. Não refere o número mínimo de participantes, pelo que se aplica o regime geral.

⁸⁸ Artigo 59º da Lei nº 81/2021, de 20 de novembro (Lei antidopagem no desporto). Exige o mesmo número de pessoas do regime geral (três). Penas: de 6 meses a 5 anos de prisão para a promoção, fundação e apoio (número 1); para a chefia ou direção a mesma pena agravada de um terço nos seus limites mínimo e máximo (número 2).

⁸⁹ Números 1 e 3 do artigo 34º da Lei n.º 37/2011, de 22 de junho (simplifica procedimentos de transmissão e circulação de produtos defesa), com penas de 4 a 12 anos de prisão.

4. Prevenção e combate ao terrorismo, ao crime organizado e ao branqueamento

4.1. União Europeia

Começamos por registar que no âmbito da Política Comum de Segurança e Defesa, resulta das disposições conjugadas do número 7 do artigo 42º com o número 1 do artigo 43º do Tratado da União Europeia que os EEMM devem auxiliar-se mutuamente em caso de agressão terrorista, dever que surge reforçado na cláusula de solidariedade ínsita na alínea *a*) do número 1 do artigo 222º do TFUE.

Continuando nos Tratados, registamos que o artigo 83º do TFUE possibilita a fixação de regras mínimas sobre as medidas de combate e as infrações penais relativas, entre outros crimes graves transfronteiriços, ao terrorismo e seu financiamento, ao crime organizado e ao branqueamento, contemplando-se nos artigos 82º a 86º do TFUE a cooperação judiciária em matéria penal e nos artigos 87º a 89º a cooperação policial.

Iniciamos com a Europol prevista no artigo 88º do TFUE cujo regime atual consta do Regulamento (UE) 2016/794 do PE e do Conselho⁹⁰ que cria a Agência da União Europeia para a Cooperação Policial a qual tem como missões apoiar e reforçar a eficácia da ação das autoridades policiais e judiciárias dos EEMM em matéria de prevenção e repressão da criminalidade grave que afete dois ou mais EEMM⁹¹, e outras formas de criminalidade constantes do número 1 do artigo 3º e do anexo I ao Regulamento Europol que inclui o terrorismo e seu financiamento, o crime organizado e o branqueamento⁹², que afetem um interesse comum abrangido por uma política da União⁹³.

⁹⁰ De 5 de novembro de 2016 (JO L 135, de 24 de maio de 2016). O Regulamento Europol foi antecedido pelas Convenções Europol de 1995 e de 2009.

⁹¹ Estas condições constam do artigo 3º da Convenção Europol de 2009 e da alínea *a*) do número 1 do artigo 2º da Convenção de 1995.

⁹² Este anexo I inclui outros crimes como o terrorismo, o tráfico de estupefacientes, tráfico de seres humanos, de órgãos e tecidos humanos, rapto, sequestro e tomada de reféns, racismo e xenofobia, criminalidade informática, corrupção, tráfico de armas, de espécies animais e vegetais ameaçadas, crimes contra o ambiente, abuso e exploração sexual, incluindo material relacionado com o aliciamento e abuso sexual de crianças, genocídio, crimes contra a humanidade e crimes de guerra. *Cf.*: artigo 3º da Convenção e Europol de 2009 e número 2 do artigo 2º da Convenção de 1995.

O Regulamento Europol determina no seu artigo 7º a criação por cada EEMM de uma unidade nacional para a execução das suas atribuições⁹⁴ que funciona, de acordo com o número 5 do artigo 7º como organismo de ligação entre a Europol e as autoridades nacionais competentes, destinada, nomeadamente, à transmissão de dados e informações e a assegurar a comunicação e cooperação de todas as autoridades competentes⁹⁵.

A Lei nº 53/2008, de 29 de agosto, (Lei de Segurança Interna)⁹⁶, no seu artigo 23-A atribui ao Ponto Único de Contato para a Cooperação Policial Internacional (PUC-CPI), que, de acordo com o seu número 3, funciona na dependência e sob a coordenação do Secretário-Geral do Sistema de Segurança Interna (SIS) a responsabilidade operacional pela coordenação da cooperação policial internacional⁹⁷, dispondo de um Gabinete de Gestão

⁹³ Artigo 88º. Acordo e articulação das operações da Europol com as autoridades dos EEMM afetados. Intervenção de autoridades de um EEMM no território de outro (artigo 89º). A Decisão 2009/371/JAI do Conselho de 1 de janeiro de 2010, fixa regras de segurança, controlo, confidencialidade e prazos de conservação e utilização das informações e dados pela Europol.

⁹⁴ Acerca de idênticas obrigações constantes na regulamentação Europol revogada, *cf.*: o artigo 8º da Convenção Europol de 2009 e o artigo 4º da Convenção de 1995.

⁹⁵ Número 6 do artigo 7º. Determina também a Convenção Europol a nomeação por cada unidade nacional de um agente de ligação que, designadamente, contribui para o intercâmbio de informações entre a Europol e os EEMM, países terceiros e organizações internacionais (Artigo 8º. *Cf.*: o artigo 9º da Convenção Europol de 2009 e o artigo 5º da Convenção Europol de 1995). Acerca da Europol até à Convenção de 2009, *cf.*: JOSÉ DANIEL TAVARES, «*Reflexões sobre a segurança na Europa. A EUROPOL. Da Convenção de 1995 à de 2009*», *Lusíada. Direito*, Lisboa, nº 14, 2015, pp. 7-21, sendo válidas para o regime atual a maioria das considerações formuladas a propósito do regime anterior.

⁹⁶ Na redação dada pela Lei nº 24/2022, de 16 de dezembro de 2022. *Cf.*: também o Decreto-Lei n.º 10/2020, de 11 de março de 2020 (Orgânica do Ponto Único de Contato para a Cooperação Policial Internacional (PUC-CPI), alterado pelo Decreto-Lei nº 8/2023, de 31 de janeiro.

⁹⁷ Designadamente assegurar o encaminhamento dos pedidos de informação nacionais, a receção, o encaminhamento e a difusão nacional de informação proveniente das autoridades estrangeiras, a transmissão de informação e a satisfação dos pedidos formulados por aquelas autoridades (nº 1), assegurar o intercâmbio internacional de informações entre os serviços de polícia, como referido na alínea a) do nº 2 e orientar a interlocução externa neste âmbito, garantindo a operacionalidade dos seus mecanismos e instrumentos como consta das alíneas b) e c) do número 2. *Cf.*: a Lei n.º 74/2009, de 12 de agosto de 2009 (Intercâmbio de dados e informações de natureza criminal na União Europeia).

que integra entre outros serviços, a Unidade Nacional da EUROPOL, o Gabinete Nacional da INTERPOL⁹⁸, o Gabinete de Informações de Passageiros, a coordenação dos oficiais de ligação nacionais e estrangeiros, competindo a chefia do Gabinete EUROPOL e INTERPOL ao coordenador de Gabinete da Polícia Judiciária⁹⁹.

O TFUE refere no seu artigo 85º a Eurojust – União Europeia de Cooperação Judiciária relativa à cooperação policial na investigação e ação penal da criminalidade grave que afete dois ou mais Estados incluindo o terrorismo e ao incentivo da cooperação policial entre as autoridades dos EEMM.

A Eurojust consta atualmente do Regulamento (UE) 2018/1727 do P. E. e do Conselho¹⁰⁰, sendo, em conformidade com o seu artigo 7º, destacado por cada Estado-Membro para a Eurojust um membro nacional com estatuto de procurador, de juiz ou de representante judiciário equivalente, para trabalhar na sede da Eurojust com competências para, designadamente,

⁹⁸ Número 6 do artigo 23-A da Lei nº 53/2008. No mesmo sentido se pronuncia a alínea *b*) do número 4 do artigo 2º do Decreto-Lei nº 10/2020, de 11 de março (Orgânica do ponto único de contato para a cooperação policial internacional), alterado pelo Decreto-Lei nº 8/2023, de 31 de janeiro. *Cf.*: também o artigo 12º (Cooperação Internacional) da Lei nº 49/2008, de 27 de agosto (Lei de Organização da Investigação Criminal), que refere que «[o] Ponto Único de Contato para a Cooperação Policial Internacional (PUC-CPI) é o centro operacional responsável pela coordenação da cooperação policial internacional (...) e que O PUC-CPI integra, sob a mesma gestão (...) a Unidade Nacional da EUROPOL, o Gabinete Nacional da INTERPOL». A redação do artigo 12º antes da alteração efetuada pela Lei n.º 24/2022, de 16/12 era a seguinte: «[c]ompete à Polícia Judiciária assegurar o funcionamento da Unidade Nacional EUROPOL e do Gabinete Nacional INTERPOL (nº 1).

⁹⁹ Número 8 do artigo 23-A da Lei nº 53/2008, de 29 de agosto. Anteriormente à alteração da Lei nº 53/2008, de 29 de agosto pela Lei nº 24/2022, de 16 de dezembro, a representação em Portugal da Europol e da Interpol estava a cargo da Unidade de Cooperação Internacional da Polícia Judiciária, nos termos do da alínea *a*) do nº 2 do artigo 5º e do artigo 7º e da alínea *a*), *iii*) do nº 4 do artigo 18º (Unidade de Cooperação Internacional que se mantém atualmente), conjugados com o nº 1 do artigo 38º do Decreto-Lei n.º 137/2019, de 13 de setembro (Estrutura Organizacional da Polícia Judiciária). Este preceito foi, em consequência, também alterado pelo Decreto-Lei nº 8/2023, de 31 de janeiro, estabelecendo o número 1 do artigo 7.º (cooperação policial internacional) que «[a] atribuições da PJ em matéria de cooperação policial internacional são exercidas no respeito pelo quadro legal de competências próprias do Ponto Único de Contato para a Cooperação Policial Internacional (PUC-CPI)», sendo alterado em consonância o artigo 38º. *Cf.*: ainda o artigo 27º (cooperação internacional da Unidade de Informação Financeira).

¹⁰⁰ De 14 de novembro de 2018 (JO L 295, de 21 de novembro de 2018).

facilitar ou apoiar a emissão ou a execução de pedidos de auxílio judiciário mútuo ou de reconhecimento mútuo, nos termos dos artigos 8º e 9º.

Com importância no combate ao terrorismo e ao crime organizado em geral, registamos também a Rede Judiciária Europeia em Matéria Penal¹⁰¹, relativa à existência de uma rede de pontos de contato judiciários e peritos em cooperação judiciária internacional presentes em todos os Estados da União Europeia para facilitar a cooperação judiciária internacional¹⁰².

Cumprir referir agora o Mandado de Detenção Europeu definido na Decisão-Quadro 2002/584/JAI do Conselho¹⁰³ destinado a cumprir uma decisão judiciária emitida por um EEMM para detenção e entrega por outro EEMM de um suspeito ou condenado por crimes como a participação numa organização criminosa e terrorismo.

Cabe efetuar também uma referência à Procuradoria Europeia prevista no artigo 86º do TFUE e criada pelo Regulamento (UE) 2017/1939 do Conselho¹⁰⁴ destinada a combater infrações penais lesivas dos interesses financeiros da União Europeia¹⁰⁵.

4.2 Portugal, medidas especiais de combate: registo de voz e imagem, quebra do sigilo bancário, ações encobertas e proteção de testemunhas

4.2.1. Terrorismo

Portugal criou vários mecanismos reforçados de prevenção e combate ao terrorismo e às ameaças para a paz e segurança que o mesmo representa.

¹⁰¹ *Cfr.* a alínea c) do nº 1 do artigo 85º TFUE e a Decisão 2008/976/JAI do Conselho, de 16 de dezembro de 2008 (JO L 348 de 24 de dezembro de 2008) alterada pela Decisão nº 568/2009/CE do Parlamento Europeu e do Conselho, de 18 de junho de 2009 (JO L nº 168, de 30 de junho de 2009).

¹⁰² Especialmente no crime organizado, corrupção, tráfico de estupefacientes ou terrorismo. É composta pelas autoridades judiciárias ou outras autoridades competentes com responsabilidades específicas no quadro da cooperação internacional. *Cfr.* artigo 2º.

¹⁰³ De 13 de junho de 2002 (JO L 190, de 18 de julho de 2002), alterada pela Decisão-Quadro 2009/299/JAI do Conselho de 26 de fevereiro de 2009 (JO L 81, de 27 de março de 2009).

¹⁰⁴ De 12 de outubro de 2017 (JO L 283, de 31 de outubro de 2017).

¹⁰⁵ Tais infrações constam da Diretiva (UE) 2017/1371, de 5 de julho de 2017 (JO L 198, de 28 de julho de 2017) relativa à luta contra a fraude lesiva dos interesses financeiros da União através do direito penal.

Assim, desde logo, artigo 23º da Lei nº 53/2008, de 23 de agosto (Lei de Segurança Interna) atrás identificada¹⁰⁶ cria uma Unidade de Coordenação Antiterrorismo¹⁰⁷ que integra os responsáveis máximos das diversas entidades policiais e das forças armadas, com competência na coordenação e definição de estratégias de combate ao terrorismo¹⁰⁸ à qual compete, designadamente, a coordenação e partilha de informações com vista ao combate ao terrorismo no âmbito do Sistema de Segurança Interna e a articulação entre os organismos envolvidos e a cooperação internacional.

O regime de organização e funcionamento da Unidade de Coordenação Antiterrorismo (UCAT) consta do Decreto Regulamentar nº 2/2016, de 23 de agosto, competindo-lhe, nomeadamente «a coordenação dos planos de execução das ações previstas na Estratégia Nacional de Combate ao Terrorismo¹⁰⁹ (...) e, no plano da cooperação internacional, a articulação e coordenação entre os pontos de contacto para as diversas áreas de intervenção em matéria de terrorismo», de acordo com o nº 2 do seu artigo 2º.

O Código de Processo Penal prevê a possibilidade de proteção de testemunhas, entre outros, em processos de terrorismo¹¹⁰, permitindo ainda

¹⁰⁶ Sofreu várias alterações, a última das quais pela Lei nº 24/2022, de 16 de dezembro.

¹⁰⁷ *Cfr.* também a Estratégia Nacional de Combate ao Terrorismo (Resolução do Conselho de Ministro nº 7-A/2015, de 20 de fevereiro) e a Unidade Nacional Contraterrorismo (UNCT): alínea a) do nº 3 do artigo 18º e artigo 30º do D.L. nº 137/2019, de 13 de setembro (Estrutura Organizacional da Polícia Judiciária).

¹⁰⁸ Na sequência da extinção do SEF, a Lei nº 53/2008, de 23 de agosto, sofreu alterações pela Lei 73/2021, de 12 de novembro, para entrar em vigor em 15 de maio de 2022, prazo adiado *sine die* até à criação da Agência Portuguesa para as Migrações e Asilo (APMA), prevista no seu artigo 14º-A, aditado pela Lei nº 11/2022, de 06 de maio. A referida Agência foi criada pelo D. L. nº 41/2023, de 2 de junho, extinguindo por fusão o SEF (artigos 1º a 3º conjugados com o artigo 4º do D. L. nº 40/2023, de 2 de junho, que extingue a carreira de investigação e fiscalização do SEF). Estes diplomas entraram em vigor e produzem efeitos desde 29 de outubro de 2023, por força do disposto no artigo 49º do D. L. nº 41/2023, e artigo 31º do D. L. nº 40/2023.

¹⁰⁹ Constante da Resolução do Conselho de Ministro nº 7-A/2015, de 20 de fevereiro.

¹¹⁰ Número 2 do artigo 139º/2. *Cfr.* a Lei nº 93/99, de 14 de julho (Lei de proteção de testemunhas), alterada várias vezes, a última das quais pela Lei nº 2/2023, de 16 de janeiro. Na alínea a) do seu artigo 16º permite que nos processos relativos a infrações terroristas, infrações relacionadas com um grupo terrorista, infrações relacionadas com atividades terroristas e de financiamento do terrorismo, possa ser ocultada a identidade das testemunhas desde que estas ou seus familiares possam correr perigo grave, sejam credíveis e o seu testemunho constitua um contributo probatório de relevo.

na alínea a) do nº 2 do seu artigo 177º várias medidas como a realização de buscas domiciliárias entre as 21 e as 07 horas, na alínea a) do nº 2 do artigo 187º um regime especial de autorização das escutas telefónicas, na alínea c) do nº 1 do artigo 202º a aplicação da medida de coação de prisão preventiva e, nos termos do número 2 do artigo 215º a respetiva duração.

A alínea k) do nº 2 do artigo 6º do D. L. 43/2002, de 2 de março, atribui à Autoridade Marítima Nacional competências para a «prevenção e repressão da criminalidade, nomeadamente no que concerne ao combate ao narcotráfico, ao terrorismo e à pirataria».

Por outro lado, a Lei nº 49/2008, de 27 de Agosto, de Organização da Investigação Criminal (LOIC) atribui, respetivamente nas alíneas g) e l) do nº 2 do artigo 7º, à Polícia Judiciária competência reservada indeferível noutros órgãos de polícia criminal (OPC's) para a investigação criminal de crimes como os de associação criminosa e de «infrações terroristas, infrações relacionadas com um grupo terrorista, infrações relacionadas com atividades terroristas e financiamento do terrorismo», cabendo ainda registar que na Estrutura Orgânica da PJ, plasmada no Decreto Lei nº 137/2019, de 13 de Setembro¹¹¹ se prevê a recolha e tratamento de informações pela sua Unidade de Informação Financeira referentes ao branqueamento e financiamento ao terrorismo prevista no artigo 27º, contemplando-se na alínea a) do nº 3 do artigo 18º e artigo 30º uma Unidade Nacional Contraterrorismo (UNCT) competente nas áreas do terrorismo, terrorismo internacional, financiamento do terrorismo e do ciberterrorismo¹¹².

Salienta-se ainda que os crimes relativos a infrações terroristas, infrações relacionadas com um grupo terrorista, infrações relacionadas com atividades terroristas e financiamento do terrorismo integram o catálogo de crimes em cuja prevenção, investigação e combate as autoridades podem recorrer a meios mais fortes e limitadores dos direitos, liberdades e garantias, como o registo de voz e imagem, a quebra do sigilo bancário e fiscal e a perda de bens e instrumentos a favor do Estado de acordo com a alínea b) do nº 1 do artigo 1º e artigos 2º a 12º da Lei nº 5/2002, de 11 de janeiro.

Na investigação dos mesmos tipos de crime é possível o recurso a ações encobertas de acordo com a alínea f) do artigo 2º da Lei nº 101/2001, de

¹¹¹ Foi alvo de diversas alterações, a última das quais pelo D. L. n.º 8/2023, de 31 de janeiro.

¹¹² Em articulação com Unidade Nacional de Combate ao Cibercrime e à Criminalidade Tecnológica (artigo 33º).

25 de agosto, considerando-se como tal, em conformidade com o nº 2 do artigo 1º «aquelas que sejam desenvolvidas por funcionários de investigação criminal ou por terceiro atuando sob o controlo da Polícia Judiciária para prevenção ou repressão dos crimes indicados na Lei nº 101/2001, de 25 de agosto, com ocultação da sua qualidade e identidade», competindo igualmente à Polícia Judiciária a responsabilidade pela gestão das identidades fictícias, conforme previsto no nº 5 do artigo 5º.

Referimos finalmente a Lei n.º 21/2019, de 25 de fevereiro, que regula a transferência dos dados dos registos de identificação dos passageiros (pelas companhias aéreas) transpondo a Diretiva (UE) 2016/681 do PE e do Conselho, de 27 de abril de 2016.

4.2.2. Crime organizado e branqueamento

Começamos por registar que os crimes de associação criminosa e de branqueamento constituem, de acordo com a alínea m) do artigo 1º do Código de Processo Penal, condutas que integram o conceito de criminalidade altamente organizada, preceito que reveste natureza operativa legitimando o uso de meios mais agressivos na respetiva prevenção, investigação e repressão.

A investigação dos crimes de associação criminosa (crime organizado) e de branqueamento é igualmente de reserva de competência indeferível da Polícia Judiciária nos termos das alíneas g) e i) do nº 2 do artigo 7º da Lei nº 49/2008, de 27 de agosto, sendo também aplicáveis a ambos os tipos de crime as excecionais medidas de combate previstas na Lei nº 5/2002, de 11 de janeiro, conforme previsto no respetivo âmbito de aplicação constantes das alíneas i) e j) do nº 1 do artigo 1º, possibilitando-se também o recurso a ações encobertas de acordo com as alíneas j) e m) do artigo 2º da Lei nº 101/2001, de 25 de agosto.

A Lei 83/2017, de 18 de agosto¹¹³, estabelece medidas especiais de prevenção e combate ao branqueamento de capitais e ao financiamento do terrorismo transpondo para a ordem jurídica interna as Diretivas 2015/849/UE

¹¹³ Foi alvo de várias alterações das quais a última através da Lei n.º 99-A/2021, de 31 de dezembro.

do P.E. e do Conselho e 2016/2258/UE do Conselho, prevenindo a utilização do sistema financeiro e das atividades e profissões especialmente designadas para efeitos de branqueamento de capitais e de financiamento do terrorismo¹¹⁴.

O regime promove o envolvimento na prevenção de entidades privadas (financeiras e não financeiras), junto das quais a tentativa de branqueamento possa ocorrer, através de medidas de natureza preventiva.

Tais medidas concretizam-se, entre outras, na obrigação de essas entidades procederem diligentemente à identificação dos clientes (artigos 11º e 23º), recusarem efetuar operações suspeitas (artigo 50º), conservarem documentos (artigo 51º), examinarem condutas suspeitas (artigo 52º) e comunicarem às autoridades as suspeitas de operações de branqueamento (artigos 43º a 46º).

Entre as entidades financeiras obrigadas incluem-se instituições de crédito, instituições de pagamento, sociedades de investimento mobiliário e sociedades de investimento imobiliário, empresas e mediadores de seguros que exerçam atividades no âmbito do ramo vida (alínea k) do nº 1 do artigo 3º) e entre as entidades não financeiras encontram-se concessionários de exploração de jogo em casinos e de salas do jogo do bingo, entidades pagadoras de prémios de apostas ou lotarias, entidades abrangidas pelo regime jurídico dos jogos e apostas online, comerciantes que transacionem bens ou prestem serviços cujo pagamento seja feito em numerário (artigo 4º), conservadores e oficiais dos registos (artigo 7º), solicitadores, notários, advogados e outros profissionais independentes da área jurídica constituídos em sociedade ou em prática individual (alínea f) do nº 1 do artigo 4º).

4.2.3. O Tribunal Europeu dos Direitos do Homem e o dever de denúncia dos advogados

Relativamente à obrigação que recai sobre os advogados de denunciarem as operações dos seus clientes suspeitas de branqueamento, o Tribunal Europeu dos Direitos do Homem (TEDH), embora considerando que o sigilo profissional dos advogados é fundamental na administração da justiça,

¹¹⁴ Esta legislação cumpre também a obrigação imposta aos Estados pelo disposto na alínea a) do nº 1 do artigo 7º da Convenção das Nações Unidas contra a Criminalidade Organizada Transnacional.

afirma que este não é intangível devendo ser ponderado face à luta contra o branqueamento, declarando por unanimidade que a obrigação dos advogados de denunciar, através do Presidente da Ordem dos Advogados que funciona como filtro protetor, as operações dos seus clientes suspeitas de branqueamento só respeita a atividades distantes da defesa, quando participam em nome dos seus clientes em transações financeiras, não violando o artigo 8º da Convenção Europeia dos Direitos do Homem (Direito ao respeito pela vida privada e familiar) cuja violação foi invocado pelo advogado francês Patrick Michaud¹¹⁵.

5. Conclusões

I. O terrorismo, associado ao branqueamento e à generalidade do crime organizado, ameaça gravemente a paz, a liberdade e a segurança dos cidadãos e dos Estados, bem como toda a estrutura de vida em sociedade;

II. A globalização aumenta tal ameaça que só poderá ser eficazmente combatida através de uma sólida cooperação internacional;

III. A comunidade internacional vem celebrando tratados e outros instrumentos internacionais globais, regionais e bilaterais com vista a combater tal ameaça;

IV. Acompanhando os esforços internacionais, Portugal dispõe também de legislação e estruturas para enfrentar o problema;

V. Estando em causa a própria soberania dos Estados, necessária se torna uma colaboração assente numa real vontade de partilha de preocupações, soluções, poderes, competências e meios.

¹¹⁵ Acórdão *Patrick Michaud c. França*, nº 12323/11, de 6 de dezembro de 2012. O processo teve como antecedente interno a impugnação pelo advogado francês Patrick Michaud da legislação francesa que transpôs a legislação comunitária que criou essa obrigação. Não tendo provimento nos tribunais franceses, dirigiu-se ao TEDH. O referido acórdão do TEDH encontra-se disponível em URL://hudoc.echr.coe.int/fre?i=001-115377 (consulta feita em 28 de julho de 2023).

Bibliografia

- AAVV, Jorge FIGUEIREDO DIAS (dir.), *Comentário Conimbricense do Código Penal*, Coimbra Editora, 1999
- ALBUQUERQUE, Paulo PINTO DE, “O crime de Organização Criminosa no Código Penal Português”, in Ambos, K e Romero, E. (coordenadores), *Crime Organizado, Análise da lei 12.850/2013*, Marcial Pons, São Paulo, 2017, pp. 279-289
- ALBUQUERQUE, Paulo PINTO DE., *Comentário do Código Penal à luz da Constituição da República e da Convenção Europeia dos Direitos do Homem*, 4ª ed., Universidade Católica Editora, Lisboa, 2021
- BAUER, A. e RAUFER, X., *A Globalização do Terrorismo*, Prefácio, Lisboa, 2003
- BRAZ, José., *Investigação Criminal, A Organização, o Método e a Prova. Os Desafios da Nova Criminalidade*, 5ª ed., Almedina, Coimbra, 2020
- CARRAPIÇO, Helena, *O Crime Organizado Transnacional na Europa: Origens, Práticas e Consequências*, Instituto de Defesa Nacional, Lisboa, 2006
- GARAPON, Antoine., *Crimes que não se podem punir nem perdoar*, Instituto Piaget, Lisboa, 2004 [trad. Pedro Henriques]
- GONÇALVES, Manuel MAIA., *Código Penal Português Anotado e Comentado*, 16ª ed., Almedina, Coimbra, 2004
- GOUVEIA, Jorge BACELAR, *Direito Internacional Penal. Uma Perspetiva Dogmático-Crítica*, Almedina, Coimbra, 2008
- MACHADO, Jónatas, *Direito Internacional, do Paradigma Clássico ao pós-11 de setembro*, 4ª ed., Coimbra Editora, Coimbra, 2013
- RODRIGUES, Anabela MIRANDA e MOTA, José Luís LOPES da, *Para uma Política Criminal Europeia*, Coimbra Editora, Coimbra, 2002
- TAVARES, José Daniel, “Reflexões sobre a segurança na Europa. A EUROPOL. Da Convenção de 1995 à de 2009”, *Lusitana. Direito*, nº 14, 2015, pp. 7-21
- TAVARES, José Daniel, “Fragilidade do Estado face ao Crime Organizado: A Cooperação Internacional – Uma Perspetiva Normativa”, in Pureza, J. M. e Juste Ruiz, J. (coordenadores), *Os Estados e a Ordem Internacional Contemporânea*, Imprensa da Universidade de Coimbra, Coimbra. 2019, pp. 311-330

Derecho Internacional Humanitario, Derecho Internacional de los Derechos Humanos y lucha contra el terrorismo: estudio de las normas convencionales de aplicación

International Humanitarian Law, International Human Rights Law and the fight against terrorism: a study of the conventional norms of application

Juan-Bautista Cartes Rodríguez

Resumen: Ante la escasez de estudios doctrinales sobre la materia, el presente escrito tiene por objeto un análisis detallado de la articulación entre las normas convencionales de lucha contra el terrorismo, el DIH y el DIDH. A tal fin, atenderemos a las referencias al Derecho Internacional Humanitario y a los Derechos Humanos en los tratados sectoriales de lucha contra el terrorismo –tanto de ámbito universal como regional–, para, seguidamente, hacer lo propio con las menciones al terrorismo en los tratados de Derecho Internacional Humanitario y de Derechos Humanos. De nuestro análisis se deriva que en un número significativo de tratados sectoriales se omite una referencia comprensiva al respecto, por lo que instamos a que dicha situación sea solventada.

Abstract: Given the scarcity of doctrinal studies on the subject, the purpose of this paper is to conduct a detailed analysis of the articulation of conventional anti-terrorism norms with IHL and IHRL. To this end, we will consider the references to International Humanitarian Law and Human Rights in sectoral treaties on the fight against terrorism – both universal and regional–, and then do the same with references to terrorism in treaties on International Humanitarian Law and Human Rights. Our analysis shows that a significant number of sectoral treaties omit a comprehensive reference in this regard, and we therefore urge that this situation be solved.

Palabras clave: Derecho Internacional de los Derechos Humanos; Derecho Internacional Humanitario; Terrorismo; Tratados internacionales. **Keywords:** International Human Rights Law; International Humanitarian Law; international treaties; terrorism.

Sumario: 1. A modo de introducción: reflexiones sobre la articulación del Derecho Internacional Humanitario y del Derecho Internacional de los Derechos Humanos; 2. Sobre las referencias al Derecho Internacional Humanitario y a los Derechos Humanos en los tratados sectoriales de lucha contra el terrorismo; 2.1. En el plano universal; 2.2. Y en el plano regional; 3. La contraparte: sobre la lucha contra el terrorismo en los tratados de Derecho Internacional Humanitario y de Derechos Humanos; 4. Conclusiones.

1. A modo de introducción: reflexiones sobre la articulación del Derecho Internacional Humanitario y del Derecho Internacional de los Derechos Humanos

Antes de engranar el régimen de lucha contra el terrorismo con el Derecho Internacional Humanitario (DIH) y con el Derecho Internacional de los Derechos Humanos (DIDH) hemos de realizar a título preliminar algunas apreciaciones respecto de la relación entre estos dos últimos¹. Y a

¹ Doctrinalmente, puede consultarse entre otros, LOUISE DOSWALD-BECK & SYLVAIN VITÉ, «International Humanitarian Law and Human Rights Law», *International Review of the Red Cross*, vol. 33, n° 293, 1993, pp. 94-119; HANS-JOACHIM HEINTZE, «On the Relationship Between Human Rights Law Protection and International Humanitarian Law», *International Review of the Red Cross*, vol. 86, n° 856, 2004, pp. 789-814; HEIKE KRIEGER, «A conflict of norms: the relationship between Humanitarian Law and Human Rights Law in the ICRC Customary Law Study», *Journal of Conflict and Security Law*, vol. 11, n° 2, 2006, pp. 265-291; RENE PROVOST, *International Human Rights and Humanitarian Law*, Cambridge University Press, Cambridge, 2002; OONA HATHAWAY, et. al., «Which law governs during armed conflict the relationship between International Humanitarian Law and Human Rights Law», *Minnesota Law Review*, vol. 96, n°. 6, 2012, pp. 1883-1943; JACQUES MEURANT, «Droit humanitaire et droits de l'homme: spécificités et convergences», *International Review of the Red Cross*, vol. 75, n°. 800, 1993, pp. 93-98; GLORIA GAGGIOLI, *L'influence mutuelle entre les droits de l'homme et le droit international humanitaire à la lumière du droit à la vie*, Pedone, Paris, 2013.

tal fin no podemos sino comenzar por recordar qué entendemos por ambos regímenes.

Así pues, en primer lugar, podemos definir el Derecho Internacional Humanitario como aquella rama del Derecho Internacional Público encargado de regular, por un lado, la protección de las personas que, bien no participan en las hostilidades, bien han dejado de ser partícipes en las mismas. Y, por otro, de regular qué métodos y qué medios de guerra pueden ser utilizados, y cuales, por contra, no; procurando un equilibrio entre los principios de humanidad y necesidad militar². Por su parte, el Derecho Internacional de los Derechos Humanos es aquella rama del Derecho Internacional Público enfocada en las obligaciones que han asumido los Estados en lo que atañe al respeto, protección y promoción de los derechos humanos, en virtud, principalmente, de tratados tanto universales como regionales.

Por ende, ambos sectores se enmarcan dentro del Derecho Internacional Público, y, por ende, con él comparten tanto un conjunto de normas, como un conjunto de principios que las informan. Así pues, además de las reglas de interpretación generales contempladas en los artículos 31 a 33 de la Convención de Viena sobre el Derecho de los Tratados (1969), desde una perspectiva hermenéutica en ambas ramas del ordenamiento internacional adquiere una importancia radical el principio *pro homine*. Y ello como consecuencia de que ambas ramas tienen en común la protección de la dignidad humana en tanto que última ratio. De tal suerte que como fue establecido por el Tribunal Penal Internacional para la ex-Yugoslavia:

«La esencia de todo el *corpus* del Derecho Internacional Humanitario, así como de los Derechos Humanos descansa en la protección de la dignidad humana de toda persona, cualquiera sea su género. El principio general de respeto a la dignidad humana [...] es la principal *raison d'être* del Derecho Internacional Humanitario y de los Derechos Humanos»³

² Cfr. CICR, *Derecho Internacional Humanitario*, Comité Internacional de la Cruz Roja, Ginebra, 2015, pp. 4-6.

³ Cfr. ICTY, *Prosecutor vs. Furundzija*, caso n.º IT-95-17/I-T, Sentencia del 10 de diciembre de 1998, párr. 183.

Siguiendo con nuestro razonamiento, y a diferencia de lo mantenido por un sector doctrinal, así como por distintos actores gubernamentales durante décadas, el Derecho Internacional de los Derechos Humanos no solo rige para tiempos de paz y el Derecho Internacional Humanitario para tiempos de guerra. Dicha afirmación es falaz, pues, por un lado, existe un núcleo de derechos humanos que «por ningún motivo» pueden ser objeto de suspensión (v. gr., artículo 4 del Pacto Internacional de Derechos Civiles y Políticos, 1966; artículo 15 del Convenio Europeo de Derechos Humanos, 1950; y artículo 27 Convención Americana de Derechos Humanos, 1978). Más aún, en sistemas como el africano, su tratado vertebrador, la Carta Africana de Derechos Humanos y de los Pueblos (1981), no contiene una disposición que articulada como cláusula general autorice la suspensión de ciertos derechos en tiempos de guerra o de cualquier otra situación que amenace la seguridad del Estado. De hecho, su mecanismo de garantía y control, la Comisión Africana de Derechos Humanos y de los Pueblos, ha mantenido que los Estados partes no pueden imponer ninguna restricción a cualquiera de los derechos reconocidos en el tratado (tanto civiles y políticos, como económicos, sociales y culturales) hasta el punto de que el derecho en cuestión se vuelva «ilusorio»⁴. Ello en lo que respecta al Derecho Internacional de los Derechos humanos, pero, también, algunas disposiciones del Derecho Internacional Humanitario, en concreto, «aquellas que requieren su difusión e implementación, son de aplicación en tiempos de paz»⁵. Más aún, el núcleo básico, inderogable y medular de derechos humanos presenta una coincidencia más que destacada con el contenido del artículo 3 común a los cuatro Convenios de Ginebra, así como con los artículos 75 del Protocolo I y los artículos 4 a 6 del Protocolo II⁶. Y es que de nuevo hemos de recordar que ambas ramas del Derecho internacional tienen una última ratio común.

Adicionalmente, este núcleo básico de normas se erigen en el Derecho Internacional vigente en normas imperativas o de *ius cogens*, normas que

⁴ ACHPR, Communication 140/94-141/94-145/95, *Constitutional Rights Project, Civil Liberties Organisation and Media Rights Agenda v. Nigeria*, (5 November 1999), párrs. 41 y 42.

⁵ En este sentido, cfr. ELIZABETH SALMÓN, *Introducción al Derecho Internacional Humanitario*, CICR, 2004, p. 71.

⁶ En este sentido, cfr. JUAN ANTONIO CARRILLO SALCEDO, *Soberanía de los Estados y derechos humanos en derecho internacional contemporáneo*, Tecnos, 2001, p. 68.

protegen intereses de la comunidad internacional en su conjunto y que, por ende, no admiten pacto en contrario⁷. De tal modo que con su violación, no solo se produce un hecho internacionalmente ilícito que genera la responsabilidad internacional de su autor, sino que, acudiendo al Proyecto de Artículos sobre Responsabilidad del Estado por Hechos Internacionalmente Ilícitos (2001) se despliegan una serie de consecuencias particulares; en primer lugar, cualquier Estado debe cooperar para poner fin, por medios lícitos, a toda violación grave de esta categoría de normas (art. 41.1); en segundo, ningún Estado reconocerá como lícita una situación creada por su violación ni prestará ayuda o asistencia para mantener esa situación (41.2); y en tercero, cualquier Estado podrá invocar la responsabilidad internacional del Estado autor de la violación (art. 48). Preceptos que a su vez recogen normativa consuetudinaria.

Por ende, a pesar de que ambas ramas tienen orígenes históricos distintos, a pesar de que su ámbito *ratione personae* difiere —pues el Derecho Internacional Humanitario ha de ser aplicado por las partes en el conflicto, mientras que el Derecho Internacional de los Derechos Humanos impone principalmente obligaciones a los Estados en sus relaciones con los individuos sometidos a su jurisdicción—, y a pesar de que las normas de DIH no pueden ser objeto de excepción ni suspensión, y las del DIDH (con excepciones) sí pueden serlo, de todo lo expuesto con anterioridad se deriva que el DIH y el DIDH no son ramas que nunca se articulan entre sí, sino que, por el contrario, ambos cuerpos normativos se complementan mutuamente y actúan como arterias comunicantes⁸. De hecho, cada vez son más y con mayor frecuencia los mecanismos de garantía y control de tratados de derechos humanos que se adentran y emiten pronunciamientos sobre el DIH⁹.

⁷ Art. 53, Convención de Viena sobre Derecho de los Tratados (1969).

⁸ Cuestión que ya se empezó a poner de manifiesto en la Conferencia de Teherán de 1968 sobre Derechos Humanos y que se concretó en la Declaración final de la Conferencia de las Naciones Unidas sobre Derechos Humanos de Viena de 1993.

⁹ A modo de ejemplo, en el sistema africano de derechos humanos y de los pueblos, cfr. ACHPR, *Resolution on the Promotion and Respect of International Humanitarian Law and Human and Peoples' Rights*, ACHPR/Res.7(XIV)93, 1993; *Resolution on Human Rights and Humanitarian Law Violations Resulting from Foreign Airstrikes*, ACHPR/Res.422(EXT.OS/XXVI), 2019; y en la materia que nos ocupa, ACHPR, *Resolution on the Protection of Human Rights and the Rule of Law in the Fight against Terrorism*, ACHPR/Res.88(XXXVIII)05, 2005.

De tal suerte que una vez evidenciada la articulación entre el DIH y el DIDH, dedicaremos las siguientes páginas del presente escrito al estudio de la conexión entre estos dos regímenes con el de la lucha contra el terrorismo.

2. Sobre las referencias al Derecho Internacional Humanitario y a los Derechos Humanos en los tratados sectoriales de lucha contra el terrorismo

Ya desde el año 2000 se ha venido negociando en el marco de la Sexta Comisión de la Asamblea General de la ONU un proyecto de convención general sobre el terrorismo¹⁰. No obstante, uno de los escollos más acusados a los que se está enfrentando la adopción de este instrumento es, precisamente, su articulación con el DIH y con el DIDH¹¹.

Por ende, ante la ausencia de un tratado general que regule la lucha contra el terrorismo – y ante la ausencia de un consenso sobre una definición de terrorismo – en el Derecho Internacional vigente contamos con un enfoque convencional sectorial estructurado en dos niveles: universal y regional. A continuación, seguiremos dicho criterio diferenciador para llevar a cabo el respectivo análisis jurídico.

2.1. En el plano universal...

Comenzando a nivel universal, en la actualidad nos encontramos con 19 tratados internacionales en la materia que nos ocupa:

¹⁰ Al respecto, puede consultarse, entre otros, AGNU, «Documento de trabajo presentado por la India en relación con el proyecto de convención general sobre el terrorismo internacional», Medidas para eliminar el terrorismo internacional. Informe del Grupo de Trabajo. Quincuagésimo quinto período de sesiones. Sexta Comisión. A/C.6/55/L.2, Anexo II; JOSÉ ESCRIBANO ÚBEDA-PORTUGUÉS, «Nuevos avances y retos en la lucha contra el terrorismo», *Revista Electrónica de Estudios Internacionales*, vol. 17, 2009, pp. 1-15; JANE BOULDEN, «The United Nations General Assembly and Terrorism», in *Research Handbook on International Law and Terrorism*, Edward Elgar Publishing, Cheltenham, 2020, pp. 493-505.

¹¹ Cfr. v. gr., TRISTAN FERRARO, «Interaction and Overlap Between Counter-Terrorism Legislation and International Humanitarian Law», in *Terrorism, Counter-Terrorism and International Humanitarian Law*, 17th Bruges Colloquium 20-21 October 2016, p. 30.

(i) Convenio Sobre Infracciones y Ciertos Otros Actos Cometidos a Bordo de Aeronaves, de 14 de septiembre de 1963 y que entró en vigor el 14 de diciembre de 1963;

(ii) Convenio para la Represión del Apoderamiento Ilícito de Aeronaves, de 16 de diciembre de 1970 y que entró en vigor el 14 de octubre de 1971;

(iii) Convenio para la Represión de Actos Ilícitos Contra la Seguridad de la Aviación Civil, de 23 de septiembre de 1971 y que entró en vigor el 26 de enero de 1973;

(iv) Convención sobre la Prevención y el Castigo de Delitos Contra Personas Internacionalmente Protegidas, Inclusive los Agentes Diplomáticos, de 14 de diciembre de 1973 y que entró en vigencia el 20 de febrero de 1977;

(v) Convención Internacional Contra la Toma de Rehenes, de 17 de diciembre de 1979 y que entró en vigor el 3 de junio de 1983;

(vi) Convención sobre la Protección Física de los Materiales Nucleares, de 26 de octubre de 1979 y que entró en vigor el 8 de febrero de 1987;

(vii) Protocolo para la Represión de Actos Ilícitos de Violencia en los Aeropuertos que Presten Servicios a la Aviación Civil Internacional, complementario del Convenio para la Represión de Actos Ilícitos Contra la Seguridad de la Aviación Civil, de 24 de febrero de 1988 y que entró en vigor el 6 de agosto de 1989;

(viii) Convenio para la Represión de Actos Ilícitos Contra la Seguridad de la Navegación Marítima, adoptado el 10 de marzo de 1988 y en vigor desde el 1 de marzo de 1992;

(ix) Protocolo para la Represión de Actos Ilícitos Contra la Seguridad de las Plataformas Fijas Emplazadas en la Plataforma Continental, adoptado el 10 de marzo de 1988 y en vigor desde el 1 de marzo de 1992;

(x) Convenio sobre la Marcación de Explosivos Plásticos para los Fines de Detección, adoptado el 1 de marzo de 1991 y que entró en vigor el 21 de junio de 1998;

(xi) Convenio Internacional para la Represión de los Atentados Terroristas Cometidos con Bombas, de 15 de diciembre de 1997 y que entró en vigor el 23 de mayo de 2001;

(xii) Convenio Internacional para la Represión de la Financiación del Terrorismo, de 9 de diciembre de 1999 y que entró en vigor el 10 de abril de 2002;

(xiii) Convenio Internacional para la Represión de los Actos de Terrorismo Nuclear, firmado el 13 de Abril del 2005 y que entró en vigor el 7 de Julio del 2007;

(xiv) Enmiendas a la Convención sobre la Protección Física de los Materiales Nucleares, de 8 de Julio del 2005 y que entró en vigor el 8 de mayo de 2016;

(xv) Protocolo del Convenio para la Represión de Actos Ilícitos Contra la Seguridad de la Navegación Marítima, de 14 de octubre de 2005;

(xvi) Protocolo del Protocolo para la Represión de Actos Ilícitos Contra la Seguridad de las Plataformas Fijas Emplazadas en la Plataforma Continental, de 14 de octubre del 2005;

(xvii) Convenio para la Represión de Actos Ilícitos Relacionados con la Aviación Civil Internacional, de 10 de septiembre de 2010 y en vigor el 1 de julio de 2018;

(xviii) Protocolo Complementario del Convenio para la Represión del Apoderamiento Ilícito de Aeronaves, de 10 de septiembre de 2010 y en vigor el 1 de enero de 2018;

(xix) Protocolo que modifica el Convenio sobre las Infracciones y Ciertos Otros Actos Cometidos a Bordo de las Aeronaves, de 4 de abril de 2014, en vigor el 1 de enero de 2020¹².

Sin embargo, hemos de poner de manifiesto que, de entre ellos, el primer tratado que menciona de manera expresa el concepto de derechos humanos es la Convención Internacional contra la Toma de Rehenes (1979). Concretamente en su Preámbulo, donde se establece que el mismo es adoptado “reconociendo en particular que todo individuo tiene derecho a la vida, a la libertad y a la seguridad de la persona, como se establece en *la Declaración Universal de Derechos Humanos y en el Pacto Internacional de Derechos Civiles y Políticos*”¹³. Si bien a lo largo de su articulado se omite toda referencia a dicho concepto¹⁴.

El siguiente tratado donde aparece una referencia expresa a «derechos humanos» lo encontramos en el Convenio para la Represión de Actos Ilícitos contra la Seguridad de la Navegación Marítima (1988). Nuevamente sólo en su Preámbulo, pero en dos párrafos diferentes: en el tercero, al afirmar que la Convención es adoptada «reconociendo en particular que todo individuo

¹² Todos ellos pueden ser objeto de consulta en: <https://www.refworld.org/docid/49f58cee2.html> (fecha de consulta: 15.12.2023).

¹³ Énfasis añadido.

¹⁴ Téngase en cuenta que en el presente epígrafe de este escrito van a ser analizadas las referencias a los términos «derecho humanitario» y «derechos humanos».

tiene derecho a la vida, a la libertad y a la seguridad de su persona, como se establece en la *Declaración Universal de Derechos Humanos y en el Pacto Internacional de Derechos Civiles y Políticos*», y en su párrafo octavo, donde se hace alusión a la Resolución 40/1961 de la Asamblea General de las Naciones Unidas, del 9 de diciembre de 1985, en la que «se insta a todos los Estados [...] a que presten especial atención a todas las situaciones, incluidos el colonialismo y el racismo, *así como aquellas en que haya violaciones masivas y patentes de los derechos humanos* y las libertades fundamentales, o las de ocupación extranjera, que puedan dar origen al terrorismo internacional»¹⁵.

Casi una década hubo de transcurrir para que un nuevo tratado recogiera una alusión expresa a «derechos humanos», concretamente el Convenio Internacional para la Represión de los Atentados Terroristas Cometidos con Bombas (1997). De hecho, este es el primer tratado universal que recepciona en su articulado dicho concepto. Así pues, atendiendo a su artículo 14, toda persona detenida o encausada de conformidad con el referido tratado habrá de disfrutar de todos los derechos y garantía reconocidas en «la legislación del Estado en cuyo territorio se encuentre y [en] las disposiciones pertinentes del Derecho Internacional, incluido *el Derecho Internacional en materia de derechos humanos*»¹⁶. Más aún, dicho Convenio también se caracteriza por recoger por primera vez una alusión expresa al concepto de Derecho Internacional Humanitario en su artículo 19, tanto en su primer apartado como en su segundo. Así pues, atendiendo al primero, se establece que «nada de lo dispuesto en el presente Convenio menoscabará los derechos, las obligaciones y las responsabilidades de los Estados y de los individuos con arreglo al Derecho Internacional, en particular los propósitos y principios de la Carta de las Naciones Unidas y *el Derecho Internacional Humanitario*». Mientras que en su segundo, articulado como cláusula de exclusión e incidiendo en lo establecido en el primer apartado, se recoge que «las actividades de las fuerzas armadas durante un conflicto armado, según se entienden esos términos en el *Derecho Internacional Humanitario* y que se rijan por ese derecho, no estarán sujetas al presente Convenio»¹⁷.

¹⁵ Énfasis añadido.

¹⁶ Énfasis añadido.

¹⁷ Énfasis añadido.

Una dicción similar al anterior tratado lo encontramos en el Convenio Internacional para la Represión de la Financiación del Terrorismo (1999). Así pues, en su artículo 17 se establece que toda persona detenida, encausada o respecto de la que se adopte cualquier otra medida de conformidad con el referido tratado habrá de disfrutar de todos «los derechos y garantías de conformidad con la legislación del Estado en cuyo territorio se encuentre y con las disposiciones pertinentes del Derecho Internacional, incluido *el Derecho Internacional en materia de derechos humanos*»¹⁸. Mientras que en su artículo 21 se establece que «nada de lo dispuesto en el presente Convenio menoscabará los derechos, las obligaciones y las responsabilidades de los Estados y de las personas con arreglo al Derecho Internacional y en particular [...] *el Derecho Internacional Humanitario*»¹⁹.

Por su parte, en el Convenio Internacional para la Represión de los Actos de Terrorismo Nuclear (2005) se reitera, respectivamente, en sus artículos 4.1 y 4.2, las disposiciones de Derecho Internacional Humanitario reflejadas en el Convenio Internacional para la Represión de los Atentados Terroristas Cometidos con Bombas (1997). Mientras que en materia de derechos humanos en su artículo 12 se reitera lo establecido tanto en el Convenio Internacional para la Represión de los Atentados Terroristas Cometidos con Bombas (1997) como en el Convenio Internacional para la Represión de la Financiación del Terrorismo (1999)²⁰.

Por su parte, en el artículo 1A de las Enmiendas a la Convención sobre la Protección Física de los Materiales Nucleares (2005) se recogen las mismas alusiones al Derecho Internacional Humanitario establecidas en el convenio anterior²¹, si bien, ninguna mención expresa a los derechos humanos.

¹⁸ Énfasis añadido.

¹⁹ Énfasis añadido.

²⁰ Así pues, de conformidad con el referido artículo 12, «toda persona que se encuentre detenida o respecto de la cual se adopte cualquier medida o sea encausada con arreglo al presente Convenio gozará de un trato equitativo, incluido el goce de todos los derechos y garantías de conformidad con la legislación del Estado en cuyo territorio se encuentre y con las disposiciones pertinentes del derecho internacional, incluido el derecho internacional en materia de derechos humanos».

²¹ Recordemos que en los preceptos que se están repitiendo se establece lo siguiente: «a) Nada de lo dispuesto en la presente Convención menoscabará los demás derechos, obligaciones y responsabilidades de los Estados Parte estipulados en el derecho internacional, en particular

Siguiendo un orden cronológico, hemos de detenernos en el Protocolo del Convenio para la Represión de Actos Ilícitos Contra la Seguridad de la Navegación Marítima (2005), tratado cuyas referencias a «derechos humanos» se incrementa considerablemente. Así pues, a diferencia de los tratados anteriores, en el primer apartado de su artículo 2 bis extiende la cláusula de exclusión, no solo al DIH, sino, también, de manera expresa, a los derechos humanos y al derecho de los refugiados, con la siguiente dicción:

«Nada de lo dispuesto en el presente Convenio afectará a los demás derechos, obligaciones y responsabilidades de los Estados y de las personas con arreglo al Derecho Internacional, en particular los propósitos y principios de la Carta de las Naciones Unidas y el Derecho Internacional sobre *derechos humanos, refugiados y humanitario*».

Mientras que en el segundo apartado, centrándose en el DIH y de manera idéntica a cláusulas analizadas en tratados anteriores, se establece que «las actividades de las fuerzas armadas durante un conflicto armado, según se entienden estos términos en el *Derecho Internacional Humanitario*, que se rijan por este derecho, no estarán sujetas al presente Convenio»²².

Más aún, incidiendo en el respeto de los derechos humanos, en el apartado décimo del artículo 8bis se índice en el hecho de que cuando un Estado Parte adopte medidas contra un buque de conformidad con la Convención, habrá de velar por la salvaguarda de la dignidad de las personas a bordo «de conformidad con las disposiciones aplicables del Derecho Internacional, incluida la *legislación internacional sobre derechos humanos*»²³. Por su parte, en el artículo 10.2 nos volvemos a encontrar con un tenor idéntico al establecido en tratados como el Convenio Internacional para la Represión de los Actos de Terrorismo Nuclear (2005)²⁴, recogándose

los propósitos y principios de la Carta de las Naciones Unidas y el *Derecho Humanitario Internacional*. b) Las actividades de las fuerzas armadas durante un conflicto armado, según se entienden estos términos en el *Derecho Humanitario Internacional*, que se rijan por este derecho, no estarán regidas por la presente Convención» (énfasis añadido).

²² Énfasis añadido.

²³ Énfasis añadido.

²⁴ Cfr. art. 12 del Convenio Internacional para la Represión de los Actos de Terrorismo Nuclear (2005). En este mismo sentido, art. 14 del Convenio Internacional para la Represión

que toda persona detenida, encausada o respecto de la que se adopte cualquier otra medida de conformidad con el referido tratado habrá de disfrutar de todos «los derechos y garantías de conformidad con la legislación del Estado en cuyo territorio se encuentre y con las disposiciones pertinentes del Derecho internacional, incluido *el Derecho Internacional en materia de derechos humanos*»²⁵.

Virando hacia el Convenio para la Represión de Actos Ilícitos Relacionados con la Aviación Civil Internacional (2010), si bien las referencias a derechos humanos son mucho más escasas, en él nos encontramos en su artículo 11 la misma dicción que en el artículo 10.2 del tratado anterior. Por su parte, en lo que respecta al DIH, nuevamente se establece, de manera similar a lo afirmado en convenios anteriores, que:

«Nada de lo dispuesto en el presente Convenio menoscabará los derechos, las obligaciones y las responsabilidades de los Estados y de las personas con arreglo al Derecho Internacional y en particular [...] el *Derecho Humanitario Internacional* [...] Las actividades de fuerzas armadas durante un conflicto armado, según se entienden esos términos en el *Derecho Humanitario Internacional* y que se rijan por ese derecho, no estarán sujetas al presente Convenio»²⁶

Por último, respecto de este análisis de los tratados universales hemos de hacer referencia al Protocolo Complementario del Convenio para la Represión del Apoderamiento Ilícito de Aeronaves (2010), donde en relación con el DIH se incluye el mismo contenido establecido en la convención anterior, y a donde remitimos²⁷. Mientras que en materia de derechos humanos se añade un tenor también reiterado en convenios anteriores, según

de los Atentados Terroristas Cometidos con Bombas (1997) y art. 17 del Convenio Internacional para la Represión de la Financiación del Terrorismo (1999).

²⁵ Énfasis añadido.

²⁶ Énfasis añadido. En este sentido, recordemos, también se pronuncian el art. 21 del Convenio Internacional para la Represión de la Financiación del Terrorismo (1999), el art. 4 del Convenio Internacional para la Represión de los Actos de Terrorismo Nuclear (2005), el art. 1A de las Enmiendas a la Convención sobre la Protección Física de los Materiales Nucleares (2005), el art. 2bis del Protocolo del Convenio para la Represión de Actos Ilícitos Contra la Seguridad de la Navegación Marítima (2005).

²⁷ Cfr. artículo 6 del Protocolo Complementario del Convenio para la Represión del Apoderamiento Ilícito de Aeronaves (2010).

el cual, toda persona detenida o encausada de conformidad con el referido tratado habrá de disfrutar de todos «los derechos y garantías de conformidad con la legislación del Estado en cuyo territorio se encuentre y con las disposiciones pertinentes del Derecho Internacional, incluido *el Derecho Internacional en materia de derechos humanos*»²⁸.

Recapitulando, de nuestro análisis se deriva que en los tratados sectoriales de ámbito universal se articulan cinco vías en lo que atañe a nuestro objeto de estudio. Así pues, existen once tratados en los que no aparece ninguna mención expresa ni al DIH, ni al DIDH; en otros dos tan solo se hace mención a tales conceptos en el preámbulo, pero no en su articulado; en uno se hace una mención expresa al DIDH y al DIH incluyendo una cláusula de exclusión general o reforzada sobre ambas materias; en cinco existe una cláusula de exclusión general respecto del DIH, pero no aparece expresamente una exclusión general en relación con el DIDH, y sí, en cambio, una cláusula específica de exclusión a este respecto; mientras que en uno existe una cláusula de exclusión general en relación con el DIH, pero, por el contrario, no se hace ninguna mención expresa al los derechos humanos²⁹.

De tal suerte que, concretando lo expuesto, no aparece ninguna mención en once tratados universales, algunos de los cuales han sido adoptado en los últimos años. En concreto, en el Convenio Sobre Infracciones y Ciertos Otros Actos Cometidos a Bordo de Aeronaves (1963); el Convenio para la Represión del Apoderamiento Ilícito de Aeronaves (1970); el Convenio para la Represión de Actos Ilícitos Contra la Seguridad de la Aviación Civil (1971); el Convención sobre la Prevención y el Castigo de Delitos Contra Personas Internacionalmente Protegidas, Inclusive los Agentes Diplomáticos (1973); el Convención sobre la Protección Física de los Materiales Nucleares (1979); el Convenio para la Represión de Actos Ilícitos Contra la Seguridad de la Navegación Marítima (1988); el Protocolo para la Represión de Actos Ilícitos Contra la Seguridad de las Plataformas Fijas Emplazadas en la Plataforma Continental (1988); el Convenio sobre la Marcación de Explosivos Plásticos para los Fines de Detección (1991); el Protocolo del Convenio para la Represión de Actos Ilícitos Contra la Seguridad de la Navegación

²⁸ Cfr. artículo 10 del Protocolo Complementario del Convenio para la Represión del Apoderamiento Ilícito de Aeronaves (2010). Énfasis añadido.

²⁹ En este sentido, remitimos a la tabla anexa al escrito.

Marítima (2005); Protocolo del Protocolo para la Represión de Actos Ilícitos Contra la Seguridad de las Plataformas Fijas Emplazadas en la Plataforma Continental (2005); y el Protocolo que modifica el Convenio sobre las Infracciones y Ciertos Otros Actos Cometidos a Bordo de las Aeronaves (2014).

Por su parte, en dos tratados solo se hace mención al concepto de derechos humanos en su preámbulo, pero no en el articulado; nos referimos a la Convención Internacional Contra la Toma de Rehenes (1979) y al Protocolo para la Represión de Actos Ilícitos de Violencia en los Aeropuertos que Presten Servicios a la Aviación Civil Internacional, complementario del Convenio para la Represión de Actos Ilícitos Contra la Seguridad de la Aviación Civil (1988).

Tan solo en un tratado aparece en su articulado un precepto que a modo de cláusula de derogación general expresamente determine que nada de lo dispuesto en la convención afectará a los derechos y obligaciones de los Estados y de las personas reconocidos tanto en el DIDH como en el DIH; nos referimos al Protocolo del Convenio para la Represión de Actos Ilícitos Contra la Seguridad de la Navegación Marítima (2005).

Por su parte, en cinco tratados sí existe una cláusula de derogación general respecto del DIH, pero no aparece expresamente una exclusión respecto al DIDH. Y si bien es cierto que en todos ellos sí se hace referencia al Derecho Internacional, por lo que habría de entenderse incluido el DIDH, no es menos cierto que resulta significativo la omisión de una mención expresa en este sentido. En todo caso, en todos ellos, de manera expresa, sí se hace referencia a que toda persona que sea detenida, encausada o sobre la que se adopte otra medida de conformidad con el respectivo tratado habrá de disfrutar de los derechos reconocidos por el DIDH. Por ende, nos encontramos ante una cláusula de exclusión o salvaguarda, pero no general, respecto a cualquier materia sobre la que regule el tratado como hace el Protocolo del Convenio para la Represión de Actos Ilícitos Contra la Seguridad de la Navegación Marítima (2005), sino específica³⁰. Tales tratados son el

³⁰ Así pues, este tipo de cláusulas podrían dejar distintos resquicios. Por ejemplo, imaginemos el supuesto en el que un Estado Parte deja de adoptar medidas tendentes a la protección de los derechos humanos. Igualmente, piénsese en un supuesto en el que es un tercer Estado el que adopta la medida restrictiva. O, por poner otro ejemplo, el precepto se refiere a

Convenio Internacional para la Represión de los Atentados Terroristas Cometidos con Bombas (1997); el Convenio Internacional para la Represión de la Financiación del Terrorismo (1999); el Convenio Internacional para la Represión de los Actos de Terrorismo Nuclear (2005); el Convenio para la Represión de Actos Ilícitos Relacionados con la Aviación Civil Internacional (2010); y el Protocolo Complementario del Convenio para la Represión del Apoderamiento Ilícito de Aeronaves (2010).

Por último, en las Enmiendas a la Convención sobre la Protección Física de los Materiales Nucleares (2005) se recoge una cláusula de exclusión general del DIH, pero no existe ninguna mención expresa al DIDH.

2.2. Y en el plano regional

También en el marco de diferentes organizaciones internacionales de ámbito regional se han ido adoptando distintas normas convencionales que tienen por objeto la lucha contra el terrorismo.

Así pues, en el marco de la Organización de Estados Americanos, nos encontramos, por un lado, con la Convención para Prevenir y Sancionar los Actos de Terrorismo Configurados en Delitos Contra las Personas y la Extorsión Conexa Cuando Estos Tengan Trascendencia Internacional de 2 de febrero de 1971, en vigor desde el 16 de octubre de 1973 y, por otro, con la Convención Interamericana Contra el Terrorismo de 3 de junio de 2002, en vigor desde el 10 de julio de 2003.

Comenzando con la primera de ellas, tan solo se hace una referencia a los derechos humanos en su Preámbulo, poniendo de manifiesto que dicha Convención ha sido adoptada teniendo en cuenta que «el respeto de los derechos fundamentales de la persona humana, reconocidos por la *Declaración Americana de Derechos y Deberes del Hombre* y la *Declaración Universal de los Derechos Humanos*, son deberes primordiales de los Estados». Mayor precisión aporta en este sentido la Convención Interamericana Contra el Terrorismo (2002), donde ya desde el Preámbulo enfatiza «que la lucha contra el terrorismo debe realizarse con pleno respeto al derecho nacional

personas individuales, por lo que también habría que plantearse qué ocurre respecto del ámbito de los derechos reconocidos a ciertos colectivos, como los pueblos.

e internacional, a los *derechos humanos...*» (párr. 8)³¹. Más aún, en el articulado de la Convención se dedica un precepto que tiene por título «Derechos humanos» (art. 15), donde se establece que nada de lo promulgado en el tratado menoscaba los derechos y obligaciones de los Estados y de las personas tanto de conformidad con el «Derecho Internacional Humanitario como del Derecho Internacional de los Derechos Humanos». Subrayándose en su último apartado que cualquier persona detenida o respecto de la cual se adopte cualquier medida de conformidad con la Convención «se le garantizará un trato justo, incluido el goce de todos los derechos y garantías de conformidad con la legislación del Estado en cuyo territorio se encuentre y las disposiciones pertinentes del derecho internacional». Precepto, recordemos, similar al establecido a nivel universal en el artículo 12 del Convenio Internacional para la Represión de los Actos de Terrorismo Nuclear (2005), en el artículo 14 del Convenio Internacional para la Represión de los Atentados Terroristas Cometidos con Bombas (1997), en el artículo 17 del Convenio Internacional para la Represión de la Financiación del Terrorismo (1999) o en el artículo 10 del Protocolo Complementario del Convenio para la Represión del Apoderamiento Ilícito de Aeronaves (2010).

En lo que atañe a Asia, en el marco de la Asociación del Asia Meridional para la Cooperación Regional ha sido adoptada, en primer lugar, la Convención sobre la Eliminación del Terrorismo de 4 de noviembre de 1987, en vigor desde el 22 de agosto de 1988, y en segundo, el Protocolo Adicional a la Convención sobre la Eliminación del Terrorismo *supra* del 6 de enero de 2004, en vigor desde el 12 de enero de 2006. Por su parte, también en el continente asiático, bajo los auspicios de la Asociación de Naciones del Asia Sudoriental (ASEAN) ha sido adoptada la Convención sobre la Lucha Contra el Terrorismo, de 13 de enero de 2007, en vigor desde el 27 de mayo de 2011. Por último, de las normas convencionales analizadas para este escrito, bajo los auspicios de la Organización de

³¹ Mientras que en el párrafo séptimo se recuerda que dicho tratado es adoptado «considerando que el terrorismo constituye un grave fenómeno delictivo que preocupa profundamente a todos los Estados Miembros, atenta contra la democracia, impide el goce de los *derechos humanos* y las libertades fundamentales, amenaza la seguridad de los Estados, desestabilizando y socavando las bases de la toda la sociedad, y afecta seriamente el desarrollo económico y social de los Estados de la región» (énfasis añadido).

Cooperación de Shanghái nos encontramos con la Convención para la Lucha Contra el Terrorismo, el Separatismo y el Extremismo, adoptada el 15 de junio de 2001 y en vigor el 29 de marzo de 2003.

De todos estos tratados adoptados en el continente asiático, hemos de referirnos al Protocolo Adicional a la Convención sobre la Eliminación del Terrorismo (2004), en cuyo artículo 19 se establece que ninguna disposición del presente Protocolo se interpretará en el sentido de que afecta otros derechos, obligaciones y responsabilidades de los Estados y de las personas en virtud del Derecho Internacional, en particular, del «Derecho Internacional Humanitario y del Derecho Internacional de los Derechos Humanos». Por ende, disposición similar al artículo 15 de la Convención Interamericana Contra el Terrorismo (2002), y a nivel universal, similar al artículo 2 del Protocolo del Convenio para la Represión de Actos Ilícitos Contra la Seguridad de la Navegación Marítima.

Por su parte, en la Convención sobre la Lucha Contra el Terrorismo de la ASEAN (2007) ya en el Preámbulo se recuerda el compromiso de proteger los derechos humanos, el Estado de derecho, así como el trato justo y el debido proceso (párr. 2). Igualmente, en su articulado nos encontramos con el artículo 8 donde se establece que a toda persona detenida o respecto de la cual se adopten otras medidas o se lleven a cabo procedimientos de conformidad con esta Convención se le garantizará un trato justo, incluido el disfrute de todos los derechos y garantías de conformidad con las leyes del Estado Parte en cuyo territorio se encuentre esa persona, así como con las disposiciones aplicables del Derecho Internacional, incluido el «Derecho Internacional de los Derechos Humanos»³². Por ende, de todos los tratados analizados, este es el único que excluye de manera expresa el DIDH, pero no el DIH. En todo caso, reiteramos que sobre la base de una interpretación teleológica, y de conformidad con lo dispuesto

³² Asimismo, también encontramos una referencia a los derechos humanos en relación con el artículo 10 (reconocimiento del estatuto de refugiado). Por ende, el artículo 8 de la referida convención se encuentra inspirado en preceptos como el artículo 14 del Convenio Internacional para la Represión de los Atentados Terroristas Cometidos con Bombas (1997), el artículo 17 del Convenio Internacional para la Represión de la Financiación del Terrorismo (1999) o el artículo 12 del Convenio Internacional para la Represión de los Actos de Terrorismo Nuclear (2005).

en el siguiente epígrafe, entendemos que el DIH ha de ser incluido a los efectos oportunos en el concepto genérico de «Derecho Internacional» del referido precepto.

Por su parte, en el marco de la Liga de los Estados Árabes ha sido adoptada la Convención Árabe para la Supresión del Terrorismo de 22 de abril de 1998, en vigor desde el 7 de mayo de 1999, y la Convención Árabe sobre la Lucha Contra el Blanqueo de Dinero y la Financiación del Terrorismo de 21 de diciembre de 2010. Mientras que en el marco de la Organización para la Cooperación Islámica ha sido adoptada la Convención sobre la Lucha Contra el Terrorismo Internacional, de 1 de julio de 1999. Y en el marco del Consejo de Cooperación de los Estados Árabes del Golfo, el Convenio sobre la Lucha Contra el Terrorismo de 4 de mayo de 2004.

De entre todas estas normas convencionales, tan solo en la Convención Árabe para la Supresión del Terrorismo (1998) se hace una breve referencia a los derechos humanos en su Preámbulo. Mismo proceder lo encontramos en la referida Convención sobre la Lucha Contra el Terrorismo Internacional (1999), donde se incide en que los actos de terrorismo suponen una violación grave de derechos humanos (párrs. segundo y décimo). En todo caso, no aparece ninguna mención al respeto del Derecho Internacional de los Derechos Humanos (tampoco al DIH) en la lucha contra el terrorismo.

Por otro lado, en el marco del Consejo de Europa nos encontramos con el Convenio Europeo sobre la Represión del Terrorismo, adoptado el 27 de enero de 1977, en vigor el 4 de agosto de 1978; el Convenio del Consejo de Europa para la Prevención del Terrorismo, adoptado el 16 de mayo del 2005, en vigor el 1 de junio del 2007; el Convenio del Consejo de Europa Relativo al Blanqueo, Seguimiento, Embargo y Comiso de los Productos del Delito y a la Financiación del Terrorismo, adoptado el 16 de mayo del 2005, en vigor el 1 de mayo del 2008; y el Protocolo Adicional al Convenio del Consejo de Europa para la Prevención del Terrorismo, adoptado el 22 de octubre del 2015, en vigor el 1 de julio del 2017.

En este sentido, hemos de esperar al Protocolo Adicional al Convenio del Consejo de Europa para la Prevención del Terrorismo (2015) en cuyo Preámbulo se establece que dicho tratado es adoptado con el fin de prevenir y erradicar el terrorismo «respetando al mismo tiempo los derechos humanos y el Estado de Derecho» (párr. tercero). A su vez, en el artículo primero se

incide en los efectos negativos de los actos de terrorismo en el pleno disfrute de los derechos humanos. Por su parte, en el artículo 8, bajo la rúbrica «Condiciones y salvaguardias» se enuncia que cada Estado Parte aplicará las disposiciones del presente Protocolo «con un pleno respeto a las obligaciones atinentes a los derechos humanos, en particular la libertad de circulación, la libertad de expresión, la libertad de asociación y la libertad de culto», según lo estipulado en el Convenio Europeo de Derechos Humanos, en el PIDCP y en otras obligaciones de Derecho Internacional.

Asimismo, continuando en el continente europeo, pero en el marco de la Unión Europea hemos de hacer referencia a la Directiva 2017/541 del Parlamento Europeo y del Consejo de 15 de marzo de 2017 relativa a la lucha contra el terrorismo y por la que se sustituye la Decisión marco 2002/475/JAI del Consejo y se modifica la Decisión 2005/671/JAI del Consejo. En dicha directiva se promulga que esta debe aplicarse teniendo en cuenta tanto el DIH como el DIDH. No obstante, curiosamente ello no aparece en su articulado como cláusula de salvaguardia, sino en su Preámbulo (párrs. 35 y 37)³³.

Acudiendo a la Unión Africana, bajo sus auspicios han sido adoptados, en primer lugar, la Convención para la Prevención y la Lucha Contra el Terrorismo, de 1 de julio de 1999, en vigor desde el 24 de mayo de 2017, y, en segundo, el Protocolo a la Convención para la Prevención y la Lucha Contra el Terrorismo, de 1 de julio de 2004. De entre tales instrumentos, solo la primera convención hace referencias al DIH y al DIDH. Así pues, su Preámbulo incide en el hecho de que el terrorismo da lugar a una violación grave de derechos humanos (párr. 10). Mientras que en el artículo 22 se afirma que ninguna disposición del convenio podrá interpretarse en el sentido de que deroga los principios del Derecho Internacional Humanitario, así como de la Carta Africana de Derechos Humanos y de los Pueblos.

Por último, hemos de añadir el Tratado de Cooperación entre los Estados Miembros de la Comunidad de Estados Independientes en la Lucha Contra

³³ Asimismo, recordemos que en el marco de la Unión Europea, por ejemplo, el *Acuerdo de Dublín de 1979* incorporó al Derecho de la UE el Convenio de 1977 del Consejo de Europa. En la actualidad nos encontramos realizando un análisis pormenorizado sobre la materia que nos ocupa en relación con la UE, por lo que nos remitimos a la futura publicación del mismo.

el Terrorismo de 4 de junio de 1999³⁴. Instrumento que no hace ninguna alusión ni al DIH ni al DIDH.

Por ende, recapitulando, hemos evidenciado que a nivel regional diez tratados no hacen ninguna referencia expresa ni al DIDH ni al DIH. Estos son, en el marco de la Asociación del Asia Meridional para la Cooperación Regional, la Convención sobre la Eliminación del Terrorismo (1987); en el marco de la Organización de Cooperación de Shanghái, la Convención para la Lucha Contra el Terrorismo, el Separatismo y el Extremismo (2001); en el marco de la Liga de los Estados Árabes, la Convención Árabe sobre la Lucha contra el Blanqueo de Dinero y la Financiación del Terrorismo (2010); en el marco del Consejo de Cooperación de los Estados Árabes del Golfo, el Convenio del sobre la Lucha Contra el Terrorismo (2004); en el marco del Consejo de Europa, el Convenio Europeo sobre la Represión del Terrorismo (1977), el Convenio del Consejo de Europa para la Prevención del Terrorismo (2005), y el Convenio del Consejo de Europa Relativo al Blanqueo, Seguimiento, Embargo y Comiso de los Productos del Delito y a la Financiación del Terrorismo (2005); en el marco de la Unión Africana el Protocolo a la Convención para la prevención y la lucha contra el terrorismo (2004); y en el marco de la Comunidad de Estados Independientes, el Tratado de Cooperación en la Lucha Contra el Terrorismo (1999)³⁵.

En tres tratados solo aparece una mención en el Preámbulo, pero no en el articulado, concretamente enfatizando la importancia del respeto y protección de los derechos humanos. Nos referimos a la Convención para Prevenir y Sancionar los Actos de Terrorismo Configurados en Delitos Contra las Personas y la Extorsión Conexa Cuando Estos Tengan Trascendencia Internacional de la Organización de Estados Americanos (1971); a la Convención Árabe para la Supresión del Terrorismo de la Liga de los Estados Árabes (1998); y a la Convención sobre la Lucha Contra el Terrorismo Internacional de la Organización para la Cooperación Islámica (1999). A

³⁴ A modo de ejemplo, de conformidad con su artículo 22, dicho tratado ha entrado en vigor, el 3 de octubre de 2000 para Tayikistán; el 5 de diciembre de 2000 para Kazajstán; el 6 de febrero de 2001 para Kirguistán; el 22 de agosto de 2001 para la República de Moldavia; el 28 de diciembre de 2001 para Armenia; el 18 de abril de 2004 para Bielorrusia; y el 13 de enero de 2005 para la Federación de Rusia.

³⁵ En este sentido, remitimos a la tabla anexa al escrito.

los que hemos de añadir la Directiva 2017/541 del Parlamento Europeo y del Consejo de 15 de marzo de 2017.

En dos tratados existen cláusulas de exclusión general tanto de DIH como de DIDH: en la Convención Interamericana Contra el Terrorismo de la Organización de Estados Americanos (2002) y en el Protocolo Adicional a la Convención sobre la Eliminación del Terrorismo de la Asociación del Asia Meridional para la Cooperación Regional (2004).

Y en otros tres tratados se articulan distintas combinaciones. Así pues, merece ser destacado que el Protocolo Adicional al Convenio del Consejo de Europa para la Prevención del Terrorismo del Consejo de Europa (2015) menciona expresamente la salvaguarda de las respectivas obligaciones de derechos humanos contraídas por los Estados en el plano internacional, pero se omite toda mención al DIH. Asimismo, en tal sentido no ha de pasar inadvertido que la convención enfatiza un listado de derechos, pero entre ellos no se encuentra la prohibición de la tortura o de los tratos inhumanos o degradantes, recordemos, norma imperativa del Derecho Internacional vigente. Igualmente, en esta categoría hemos de mencionar la Convención para la Prevención y la Lucha Contra el Terrorismo de la Unión Africana (1999), donde se establece que nada de lo dispuesto en el tratado podrá interpretarse en el sentido de que deroga los principios del DIH y de la Carta Africana de Derechos Humanos y de los Pueblos. Por ende, hemos de realizar dos apreciaciones a este respecto: en primer lugar, no se excluyen las normas sino los principios, no debiéndose equiparar las segundas con las primeras, y en relación con los DDHH solo se hace referencia a la Carta Africana, no a tratados universales, como por ejemplo sí hace el Protocolo del Consejo de Europa antes referido.

3. La contraparte: sobre la lucha contra el terrorismo en los tratados de Derecho Internacional Humanitario y de Derechos Humanos

Habiendo analizado las referencias al Derecho Internacional Humanitario y a los derechos humanos en los tratados sectoriales de lucha contra el terrorismo, para proporcionar una imagen completa de nuestro objeto de estudio no podemos sino, a continuación, virar hacia lo que es establecido en los tratados de derechos humanos y de Derecho Internacional Humanitario en lo que a terrorismo se refiere.

Así pues, en lo que respecta a tratados de derechos humanos, tras haber consultado los tratados más relevantes tanto del ámbito universal como de los ámbitos regionales europeo, interamericano y africano, tan solo hemos encontrado referencia a este respecto en el sistema africano. Concretamente, en la Carta Africana sobre Derechos Humanos y de los Pueblos de 27 de junio de 1981, en vigor desde el 21 de octubre de 1986, en cuyo artículo 33.2 se establece como obligación de los Estados partes que sus respectivos territorios no sean utilizados como base para actividades terroristas contra la población de ningún otro Estado parte. Asimismo, en el marco de este mismo sistema, concretamente en la Carta Africana de la Juventud de 2 de julio de 2006, en vigor desde el 8 de agosto de 2009, en su artículo 17 se promulga como obligación de los Estados partes establecer mecanismos para promover una cultura de paz y tolerancia entre los jóvenes que desaliente su participación en actos de violencia y terrorismo³⁶.

Ello sin perjuicio de que, como ha sido establecido en la introducción de este escrito, hay un núcleo de derechos humanos que no pueden ser objeto de suspensión por ningún motivo. Más aún, aunque el alcance *ratione loci* de los tratados de derechos humanos no es un tema pacífico³⁷, no podemos dejar de traer a colación las palabras del Comité de Derechos Humanos, órgano que ya puso de manifiesto hace décadas que:

³⁶ De hecho, como consecuencia de la importancia de la lucha contra el terrorismo en el sistema africano de derechos humanos, el Tribunal Africano de Justicia y Derechos Humanos y de los Pueblos tendrá competencia, una vez que empiece a funcionar, no solo sobre crímenes de guerra, lesa humanidad, genocidio o agresión, entre otros, sino también sobre actos de terrorismo. Al respecto puede consultarse lo ya analizado en este sentido en JUAN BAUTISTA CARTES RODRÍGUEZ, 2023, *El Sistema Judicial Africano de Protección de los Derechos Humanos. Un análisis de las demandas individuales*, Estudios Aranzadi, Aranzadi, 560 pp; «The Proposed African Criminal Chamber: An Effective Tool To End Impunity On African Soil?», *Revista Electrónica Cordobesa de Derecho Internacional Público*, 2019, pp. 1-12.

³⁷ A este respecto puede consultarse, v. gr., MARKO MILANOVIC, *Extraterritorial application of human rights treaties: law, principles, and policy*, Oxford University Press, Oxford, 2011; FONS COOMANS & MENNO KAMMINGA, *Extraterritorial application of human rights treaties*. Antwerp: Intersentia, 2004; MICHAEL DENNIS, «Application of human rights treaties extraterritorially in times of armed conflict and military occupation», *American Journal of International Law*, vol. 99, nº 1, 2005, pp. 119-141.

«El artículo 2 (1) del Pacto impone al Estado parte la obligación de respetar y garantizar los derechos “de todos los individuos que se encuentren en su territorio y sujetos a su jurisdicción”, pero ello no implica que el Estado parte en cuestión no pueda ser considerado responsable por violaciones de los derechos consagrados en el Pacto que sus agentes cometen en el territorio de otro Estado, ya sea con la aquiescencia del Gobierno de ese Estado o en oposición a él [...]. En consecuencia, sería inadmisibles interpretar la responsabilidad prevista en el artículo 2 del Pacto en el sentido de permitir a un Estado parte perpetrar violaciones del Pacto en el territorio de otro Estado que no podría perpetrar en su propio territorio»³⁸

Transitando ahora hacia el Derecho Internacional Humanitario, recordemos que esta es la rama del Derecho Internacional Público encargada de regular, por un lado, la protección de aquellas personas que, bien no participan en las hostilidades, bien han dejado de ser partícipes en las mismas. Y, por otro, de regular qué métodos y medios de guerra pueden ser utilizados, y cuales, por contra, no, procurando un equilibrio entre los principios de humanidad y necesidad militar³⁹. Por ende, la premisa de partida para que rija el Derecho internacional Humanitario es la existencia de un conflicto armado, ya sea un conflicto armado internacional (CAI) o un conflicto armado no internacional (CANI).

En la primera vertiente nos encontraríamos, en primer lugar, los supuestos de ataque armado de uno o varios Estados a otro Estado u otros Estados; en segundo, los supuestos en los que tenemos como partes en el conflicto armado a un Estado y a una Organización Internacional; y en tercero, los supuestos de pueblos que luchan contra la dominación colonial, la ocupación extranjera o contra regímenes racistas en el sentido de los artículos 1.4 y 96.3 del Protocolo I adicional a los Convenios de Ginebra de 1949 relativo a la protección de las víctimas de los conflictos armados internacionales de 1977 (en adelante, PAI). Mientras que para los CANI las partes en el conflicto son las fuerzas armadas de un Estado, por un lado, y un grupo armado organizado,

³⁸ Cfr. HRC, *Sergio Euben Lopez Burgos v. Uruguay*, Communication No. R.12/52, U.N. Doc. Supp. No. 40 (A/36/40) at 176 (1981), párr. 12.3.

³⁹ Cfr. CICR, *Derecho Internacional Humanitario*, Comité Internacional de la Cruz Roja, Ginebra, 2015, pp. 4-6.

por otro, o bien, grupos armados organizados luchando entre sí. Siempre, eso sí, que las hostilidades alcancen una requerida intensidad y los grupos armados presenten el requerido grado de organización⁴⁰.

De manera que, acudiendo a la materia que nos concierne en este escrito, toda vez que tiene lugar un conflicto armado, cualquier acto, con independencia de su naturaleza, se rige por el Derecho Internacional Humanitario, incluso si se cometen actos terroristas por una de las partes. Dicho con otras palabras, si nos encontramos ante un grupo armado (o un Estado) que lleva a cabo tácticas terroristas, ello no es óbice para determinar si nos encontramos ante un conflicto armado y, por ende, que rija el Derecho Internacional Humanitario⁴¹. Otro plano sería la respectiva responsabilidad internacional generada que se deriva de la comisión de tales actos.

De hecho, en los propios convenios de Ginebra se hace referencia de manera expresa a los actos de terrorismo. Así pues, en el artículo 33 del cuarto Convenio de Ginebra Relativo a la Protección Debida a las Personas Civiles en Tiempo de Guerra de 1949 se establece que «están prohibidos los castigos colectivos, así como toda medida de intimidación o de terrorismo».

Mientras que en el artículo 51.2 del Protocolo Adicional I se señala que «no serán objeto de ataque la población civil como tal ni las personas civiles. Quedan prohibidos los actos o amenazas de violencia cuya finalidad principal sea aterrorizar a la población civil».

Más aún, en el Protocolo Adicional II a los Convenios de Ginebra de 1949 relativo a la protección de las víctimas de los conflictos armados sin carácter internacional de 1977 (en adelante PAII) se recoge en su artículo 4 que «quedarán prohibidos en todo tiempo y lugar... los actos de terrorismo». Igualmente, en su artículo 13.2, con una dicción idéntica a la del PAI se

⁴⁰ Recordemos que la normativa de aplicación a los CANI sería el artículo 3 común a los Cuatro Convenios de Ginebra y el Protocolo Adicional II a los Convenios de Ginebra de 1949 relativo a la protección de las víctimas de los conflictos armados sin carácter internacional de 1977 (en adelante Protocolo Adicional II). Si bien este último establece una definición más restrictiva de CANI, en tanto que exige el requisito de control territorial para los grupos no estatales y, además, no rige para los conflictos armados donde las partes son exclusivamente grupos no estatales.

⁴¹ En este sentido se pronuncia, entre otros, MARCO SASSÒLI, “Legal Qualification of the Fight Against Terrorism”, in *Terrorism, Counter-Terrorism and International Humanitarian Law*, 17th Bruges Colloquium 20-21 October 2016, p. 48.

promulga que «no serán objeto de ataque la población civil como tal, ni las personas civiles. Quedan prohibidos los actos o amenazas de violencia cuya finalidad principal sea aterrorizar a la población civil».

En todo caso, queda fuera de toda duda que los actos de terrorismo son prohibidos por el DIH, pues en el artículo tercero común a los cuatro Convenios de Ginebra se enuncia que toda persona que no participe en las hostilidades –incluidos los miembros de las fuerzas armadas que hayan depuesto las armas, así como aquellas fuera de combate por herida, detención o por cualquier otra causa– serán, en todas las circunstancias, tratadas con humanidad. Prohibiéndose en cualquier tiempo y lugar, entre otros, los atentados contra la vida y la integridad corporal, torturas y tratos humillantes, toma de rehenes y atentados contra la dignidad personal. Mientras que, por ejemplo, en el párrafo cuarto del artículo 51 se prohíbe en todo caso los ataques indiscriminados, encontrándose entre ellos aquellos que pueden alcanzar indistintamente a objetivos militares y a personas civiles o a bienes de carácter civil.

Adentrándonos en dichas disposiciones, comenzando por la cuarta Convención de Ginebra en ella no aparece definido qué se ha de entender por el término terrorismo. Del mismo modo, al respecto existe muy poco debate grabado de la Conferencia Diplomática celebrada en Ginebra en 1949⁴². Asimismo, tampoco encontramos mucha más luz si atendemos a los comentarios a la cuarta Convención de Ginebra, donde escuetamente se señala que la prohibición de tales prácticas es debida a que golpean por igual a culpables e inocentes y a que se oponen a todos los principios basados en la humanidad y la justicia; de manera que, debido a la excesiva crueldad de las mismas, lejos de conseguir el efecto deseado, no hacen sino mantener viva la resistencia⁴³.

Por su parte, tampoco aparece definido el término terrorismo en el PAI. Acudiendo a los comentarios a dicho Protocolo ha sido establecido que el artículo 51 es uno de los más importantes de todo el tratado, pues

⁴² Cfr. Swiss Federal Council, *Final Record of the Diplomatic Conference of Geneva of 1949*, Federal Political Department, 1949.

⁴³ Cfr. JEAN PICTET, *Commentary of the Geneva Convention Relative to the Protection of Civilian Persons in Time of War*, International Committee of the Red Cross, 1958, pp. 225-226.

codifica la norma consuetudinaria de protección a favor de los civiles⁴⁴. No obstante, respecto de la materia que nos concierne escuetamente se señala que tal precepto:

«tiene por objeto prohibir los actos de violencia cuyo objetivo principal sea sembrar el terror entre la población civil sin ofrecer una ventaja militar sustancial. Es interesante señalar que también están prohibidas las amenazas de cometer tales actos»⁴⁵

En lo que respecta al PAII, del mismo modo, no se define el término terrorismo. Si acudimos al artículo 4, fue propuesto que se prohibiese tan solo «los actos de terrorismo en forma de actos de violencia cometidos contra [...] personas». No obstante, el enunciado finalmente adoptado es más general prohibiendo, por ejemplo, «los actos dirigidos contra instalaciones que, como efecto secundario, causarían víctimas»⁴⁶. Más aún, enlazando con el artículo 13.2 de este mismo Protocolo, en los comentarios al artículo 4 se señala que «los actos o amenazas de violencia que tienen como objetivo aterrorizar a la población civil, constituyen un tipo especial de terrorismo y son objeto de una prohibición específica». A su vez, acudiendo a los comentarios del referido artículo 13.2, en ellos se recoge que ya desde hace mucho tiempo se intenta prohibir dichos ataques por causar sufrimientos especialmente crueles y reprensibles a la población civil. De hecho, se alude a que en el Proyecto de Reglas de la Guerra Aérea (1922), ya se prohibían tales actuaciones, eso sí, limitadas a este tipo de guerras, mientras que el enunciado del PAII (así como del PAI) abarca todas las circunstancias posibles. Cabe resaltar que ni siquiera en los comentarios se pretende definir el término terrorismo y simplemente se concluye afirmando que «los ataques o amenazas de que se trata son, por tanto, aquellos cuyo objetivo principal es sembrar el terror, como afirmó un delegado durante los debates de la Conferencia»⁴⁷.

⁴⁴ Cfr. YVES SANDOZ, CHRISTOPHE SWINARSKI, BRUNO ZIMMERMANN, *Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949*, Martinus Nijhoff Publishers, International Committee of the Red Cross, Geneva, 1987, p. 615

⁴⁵ *Ibid.*, p. 618, (traducción propia).

⁴⁶ *Ibid.*, p. 1375.

⁴⁷ *Ibid.*, p. 1453. Por su parte, no ha de obviarse que en los Estatutos del Tribunal Internacional para Ruanda y del Tribunal Especial para Sierra Leona se establece que tales tribunales

En todo caso, a pesar de las limitaciones referidas, no podemos concluir el presente epígrafe sin realizar una serie de reflexiones con arreglo a los CAI y los CANI.

En lo que respecta a los CAI, se ha de subrayar que los propios Estados pueden llevar a cabo actos de terrorismo, y generarse, por ende, la respectiva responsabilidad internacional derivada de la comisión de tales actos⁴⁸. Por otro lado, tradicionalmente ha existido una corriente que excluye las actuaciones de los movimientos de liberación nacional de los actos terroristas. De hecho, en tres tratados –la Convención Árabe para la Supresión del Terrorismo de la Liga de los Estados Árabes (1998), la Convención sobre la Lucha Contra el Terrorismo Internacional de la Organización para la Cooperación Islámica (1999) y la Convención para la Prevención y la Lucha Contra el Terrorismo de la Unión Africana (1999) – se procede a excluir expresamente de su objeto de regulación las luchas de liberación nacional⁴⁹. No obstante, en estos mismos preceptos se establece que tales luchas han de conducirse de conformidad con los principios de Derecho Internacional. No debiéndose obviar que los actos terroristas, ya sean implícita, ya sean expresamente, aparecen prohibidos en el DIH vigente tal y como ha sido referido *supra*. Más aún, tales prohibiciones no solo quedan recogidas en los respectivos tratados, sino, además, en normativa consuetudinaria general⁵⁰. Así pues, tanto Estados como MLN pueden cometer actos terroristas⁵¹.

Del mismo modo, hemos de poner de manifiesto que un grupo terrorista puede ser parte de un CAI si logra establecerse como el nuevo gobierno de un Estado y entabla un conflicto armado con otro Estado; al igual que si el

tendrán competencia «para enjuiciar a las personas que cometan u ordenen la comisión de graves violaciones del artículo 3 común a los Convenios de Ginebra de 12 de agosto de 1949 relativos a la protección de las víctimas de los conflictos armados y del Protocolo Adicional II de los Convenios, de 8 de junio de 1977. Dichas violaciones comprenderán [...] *los actos de terrorismo*» (respectivamente, artículos tercero y cuarto, énfasis añadido).

⁴⁸ En este sentido resulta de interés las reflexiones de JOAQUÍN ALCAIDE FERNÁNDEZ, «¿Es Posible Atribuir Responsabilidad Internacional a los Estados Acusados de Cometer Actos Terroristas», *Derecho PUCP*, vol. 63, 2009, 203-230.

⁴⁹ Respectivamente, consúltese el artículo segundo de los dos primeros tratados y el artículo tercero del tercer tratado.

⁵⁰ CICR, *Derecho consuetudinario*, disponible en: <https://ihl-databases.icrc.org/es/customary-ihl/v1> (fecha de consulta: 15.12.2023).

⁵¹ En este mismo sentido, J. ALCAIDE FERNÁNDEZ, «¿Es Posible Atribuir...», *op. cit.*, p. 212.

grupo terrorista actúa contra otro Estado bajo el control de un segundo Estado⁵²; e incluso el reconocimiento del estatuto de beligerancia—de manera expresa o implícita— a un grupo organizado que comete actos terroristas podría situar a dicho grupo como parte de un CAI⁵³.

Por su parte, en lo que atañe a los CANI, recordemos que las partes en el conflicto son las fuerzas armadas de un Estado, por un lado, y un grupo armado organizado, por otro, o bien, grupos armados organizados luchando entre sí. Siempre eso sí, que las hostilidades alcancen una requerida intensidad y los grupos armados presenten el requerido grado de organización⁵⁴.

En todo caso, más allá de la teoría, la realidad ha evidenciado la apertura de muy distintos escenarios, por ejemplo, cuando un Estado (o varios) recurren a la fuerza armada contra un grupo terrorista que actúa desde el territorio de otro Estado, en el supuesto en el que éste último Estado no haya consentido el uso de la fuerza a este respecto. De tal suerte que ante tal escenario surge el interrogante de si resulta de aplicación las reglas relativas a los conflictos armados internacionales, la de los conflictos armados no internacionales, o ambas a la vez—en este último supuesto entendiendo que nos encontraríamos ante un conflicto armado internacional contra el Estado territorial y, de manera paralela, ante un conflicto armado no internacional

⁵² Entendemos que sería suficiente en tal sentido un «control general». A este respecto, cfr. ICRC, *Commentary on the First Geneva Convention Convention (I) for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field*, Cambridge University Press, Cambridge, 2016, p. 99; ICTY, *The Prosecutor v. Dusko Tadic*, Appeals Chamber, Merits Judgement, 15 July 1999, IT-94-1-A, párr. 131.

⁵³ En este sentido se pronuncia ROGIER BARTELS, «Terrorist Groups as Parties to an Armed Conflict», in *Terrorism, Counter-Terrorism and International Humanitarian Law*, 17th Bruges Colloquium 20-21 October 2016, p. 59. Autor que añade que «the debate that arose some years ago as to whether the Revolutionary Armed Forces of Columbia (FARC), which had been designated by many countries and international organisations as a terrorist organisation, had been recognised by Colombia as a belligerent, shows that this possibility is not entirely unrealistic».

⁵⁴ Recordemos que la normativa de aplicación a los CANI sería el artículo 3 común a los Cuatro Convenios de Ginebra y el Protocolo Adicional II a los Convenios de Ginebra de 1949 relativo a la protección de las víctimas de los conflictos armados sin carácter internacional de 1977 (en adelante Protocolo Adicional II). Si bien este último establece una definición más restrictiva de CANI, en tanto que exige el requisito de control territorial para los grupos no estatales y, además, no rige para los conflictos armados donde las partes son exclusivamente grupos no estatales.

contra el grupo armado—. Si bien hasta la fecha no es una cuestión pacífica, este último es el que parece defender actualmente la CICR⁵⁵. No obstante, no ha de pasar desapercibida la posición mantenida por autores como Sassòli y Carron, quienes mantienen que resulta de aplicación en exclusiva la normativa de Derecho Internacional Humanitario de los conflictos no internacionales sobre la base del siguiente razonamiento:

«La respuesta se puede encontrar aplicando una presunción. El uso de la fuerza contra objetivos en el territorio de un Estado que no consiente normalmente está cubierto por las disposiciones del DIH sobre conflictos armados internacionales, excepto si el uso de la fuerza tiene como objetivo exclusivo al grupo armado. [Asimismo], es evidente que el Estado territorial podría, en cualquier momento, convertir el conflicto en un conflicto armado internacional si se resiste por la fuerza a la intervención armada»⁵⁶

4. Conclusiones

De lo analizado en el presente escrito podemos afirmar que a pesar de la innegable significación del Derecho Internacional Humanitario y del Derecho Internacional de los Derechos Humanos en la lucha contra el terrorismo, la mayoría de tratados analizados obvian una mención expresa sobre la articulación de sendas ramas. Más aún, no son desdeñables los tratados que en su preámbulo sí hacen mención a dicha materia, e incluso ensalzan su importancia, pero en los que se omite toda regulación en su articulado.

Por ende, desde este escrito afirmamos la necesidad de vincular cláusulas en los tratados de lucha contra el terrorismo que establezcan nítidamente su relación con el Derecho Internacional Humanitario y con el Derecho Internacional de los Derechos Humanos, pues, de lo contrario, dichos

⁵⁵ ICRC, *Commentary on the First Geneva Convention Convention (I) for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field*, Cambridge University Press, Cambridge, 2016, pp. 257-264.

⁵⁶ Cfr. MARCO SASSÒLI, «Legal Qualification of the Fight Against Terrorism», in *Terrorism, Counter-Terrorism and International Humanitarian Law*, 17th Bruges Colloquium 20-21 October 2016, pp. 50-51; DJEMILA CARRON, *L'acte déclencheur du conflit armé international*, Genève, Schulthess/LGDJ, 2016, pp. 356-358, (traducción propia).

silencios, ambigüedades y omisiones pueden ser utilizados con fines espurios. Más aún, ahondando en tales reflexiones, a pesar de que son la minoría, no hay que desdeñar aquellos tratados, como a nivel universal el Protocolo del Convenio para la Represión de Actos Ilícitos Contra la Seguridad de la Navegación Marítima (2005), y a nivel regional, el Protocolo Adicional a la Convención sobre la Eliminación del Terrorismo de la Asociación del Asia Meridional para la Cooperación Regional (2004), y la Convención Interamericana Contra el Terrorismo de la Organización de los Estados Americanos (2002), que expresamente y sin dejar ningún resquicio de duda establecen que nada de lo dispuesto en el respectivo tratado se interpretará en el sentido de que menoscaba los derechos y obligaciones de los Estados y de las personas conforme al DIH y al DIDH.

Así pues, si bien el primer tratado sectorial de lucha contra el terrorismo donde se contiene una mención expresa a sendas ramas –el Convenio Internacional para la Represión de los Atentados Terroristas Cometidos con Bombas (1997)– fue adoptado hace más de 25 años, el presente estudio evidencia que aún queda un largo camino por recorrer.

De hecho, como ha llegado a poner de manifiesto distintos órganos y organismos de las Naciones Unidas, en las últimas décadas, en la pretendida lucha contra el terrorismo se están cometiendo muy significativas violaciones de derechos humanos y de Derecho Internacional Humanitario⁵⁷. De tal suerte que ante tal escenario sostenemos que el respeto y protección del DIDH y del DIH no ha de ser entendido como una cortapisa para la consecución de la seguridad nacional e internacional, sino que, por el contrario, precisamente con su salvaguardia se reafirma el Estado de Derecho en el que aspiramos a vivir, se previene radicalismos, y se refuerza el círculo virtuoso de paz, lucha contra la impunidad, estabilidad y desarrollo económico, social y cultural.

Sin duda, nuestra actuación y respuesta frente a las deleznable actuaciones terroristas va determinar cómo se erige la comunidad internacional del presente y del futuro; una comunidad internacional que no se puede permitir traicionar en su recorrido a sus principios fundamentales y a sus valores aspiracionales bajo una pretendida justificación de la consecución de los mismos.

⁵⁷ Al respecto y a modo de ejemplo nos remitimos a toda la información contenida en: <https://www.ohchr.org/en/special-procedures/sr-terrorism> (fecha de consulta: 15.12.2023).

**REFERENCIAS EXPRESAS AL DERECHO INTERNACIONAL HUMANITARIO
Y A LOS DERECHOS HUMANOS EN LOS TRATADOS SECTORIALES
DE LUCHA CONTRA EL TERRORISMO**

TRATADOS SECTORIALES SOBRE TERRORISMO DE ÁMBITO UNIVERSAL	DERECHO INTERNACIONAL HUMANITARIO	DERECHO INTERNACIONAL DE LOS DERECHOS HUMANOS
Convenio Sobre Infracciones y Ciertos Otros Actos Cometidos a Bordo de Aeronaves (1963)	Ninguna mención expresa	Ninguna mención expresa
Convenio para la Represión del Apoderamiento Ilícito de Aeronaves (1970)	Ninguna mención expresa	Ninguna mención expresa
Convenio para la Represión de Actos Ilícitos Contra la Seguridad de la Aviación Civil (1971)	Ninguna mención expresa	Ninguna mención expresa
Convención sobre la Prevención y el Castigo de Delitos Contra Personas Internacionalmente Protegidas, Inclusive los Agentes Diplomáticos (1973)	Ninguna mención expresa	Ninguna mención expresa
Convención Internacional Contra la Toma de Rehenes (1979)	Ninguna mención expresa	Solo mención en Preámbulo
Convención sobre la Protección Física de los Materiales Nucleares (1979)	Ninguna mención expresa	Ninguna mención expresa
Protocolo para la Represión de Actos Ilícitos de Violencia en los Aeropuertos que Presten Servicios a la Aviación Civil Internacional, complementario del Convenio para la Represión de Actos Ilícitos Contra la Seguridad de la Aviación Civil (1988)	Ninguna mención expresa	Solo mención en Preámbulo
Convenio para la Represión de Actos Ilícitos Contra la Seguridad de la Navegación Marítima (1988)	Ninguna mención expresa	Ninguna mención expresa
Protocolo para la Represión de Actos Ilícitos Contra la Seguridad de las Plataformas Fijas Emplazadas en la Plataforma Continental (1988)	Ninguna mención expresa	Ninguna mención expresa

Convenio sobre la Marcación de Explosivos Plásticos para los Fines de Detección (1991)	Ninguna mención expresa	Ninguna mención expresa
Convenio Internacional para la Represión de los Atentados Terroristas Cometidos con Bombas (1997)	Cláusula de exclusión general	Cláusula de exclusión particular*
Convenio Internacional para la Represión de la Financiación del Terrorismo (1999)	Cláusula de exclusión general	Cláusula de exclusión particular*
Convenio Internacional para la Represión de los Actos de Terrorismo Nuclear (2005)	Cláusula de exclusión general	Cláusula de exclusión particular*
Enmiendas a la Convención sobre la Protección Física de los Materiales Nucleares (2005)	Cláusula de exclusión general	Ninguna mención expresa
Protocolo del Convenio para la Represión de Actos Ilícitos Contra la Seguridad de la Navegación Marítima (2005)	Cláusula de exclusión general	Cláusula de exclusión general
Protocolo del Protocolo para la Represión de Actos Ilícitos Contra la Seguridad de las Plataformas Fijas Emplazadas en la Plataforma Continental (2005)	Ninguna mención expresa	Ninguna mención expresa
Convenio para la Represión de Actos Ilícitos Relacionados con la Aviación Civil Internacional (2010)	Cláusula de exclusión general	Cláusula de exclusión particular*
Protocolo Complementario del Convenio para la Represión del Apoderamiento Ilícito de Aeronaves (2010)	Cláusula de exclusión general	Cláusula de exclusión particular*
Protocolo que modifica el Convenio sobre las Infracciones y Ciertos Otros Actos Cometidos a Bordo de las Aeronaves (2014)	Ninguna mención expresa	Ninguna mención expresa

*Teniendo en cuenta las apreciaciones realizadas en el presente escrito.
Fuente: elaboración propia.

**REFERENCIAS EXPRESAS A LA LUCHA CONTRA EL TERRORISMO
EN LOS TRATADOS DE DERECHO INTERNACIONAL HUMANITARIO
Y DE DERECHOS HUMANOS**

TRATADOS SECTORIALES SOBRE TERRORISMO DE ÁMBITO REGIONAL	DERECHO INTERNACIONAL HUMANITARIO	DERECHO INTERNACIONAL DE LOS DERECHOS HUMANOS
Organización de los Estados Americanos		
Convención para Prevenir y Sancionar los Actos de Terrorismo Configurados en Delitos Contra las Personas y la Extorsión Conexa Cuando Estos Tengan Trascendencia Internacional (1971)	Ninguna mención expresa	Solo mención en Preámbulo
Convención Interamericana Contra el Terrorismo (2002)	Cláusula de exclusión general	Cláusula de exclusión general
Asociación del Asia Meridional para la Cooperación Regional		
Convención sobre la Eliminación del Terrorismo (1987)	Ninguna mención expresa	Ninguna mención expresa
Protocolo Adicional a la Convención sobre la Eliminación del Terrorismo (2004)	Cláusula de exclusión general	Cláusula de exclusión general
Asociación de Naciones del Asia Sudoriental		
Convención sobre la Lucha Contra el Terrorismo (2007)	Ninguna mención expresa*	Cláusula de exclusión particular
Organización de Cooperación de Shanghái		
Convención para la Lucha Contra el Terrorismo, el Separatismo y el Extremismo (2001)	Ninguna mención expresa	Ninguna mención expresa
Liga de los Estados Árabes		
Convención Árabe para la Supresión del Terrorismo (1998)	Ninguna mención expresa	Solo mención en Preámbulo
Convención Árabe sobre la Lucha contra el Blanqueo de Dinero y la Financiación del Terrorismo (2010)	Ninguna mención expresa	Ninguna mención expresa

Organización para la Cooperación Islámica		
Convención sobre la Lucha Contra el Terrorismo Internacional (1999)	Ninguna mención expresa	Solo mención en Preámbulo
Consejo de Cooperación de los Estados Árabes del Golfo		
Convenio sobre la Lucha Contra el Terrorismo (2004)	Ninguna mención expresa	Ninguna mención expresa
Consejo de Europa		
Convenio Europeo sobre la Represión del Terrorismo (1977)	Ninguna mención expresa	Ninguna mención expresa
Convenio del Consejo de Europa para la Prevención del Terrorismo (2005)	Ninguna mención expresa	Ninguna mención expresa
Convenio del Consejo de Europa Relativo al Blanqueo, Seguimiento, Embargo y Comiso de los Productos del Delito y a la Financiación del Terrorismo (2005)	Ninguna mención expresa	Ninguna mención expresa
Protocolo Adicional al Convenio del Consejo de Europa para la Prevención del Terrorismo (2015)	Ninguna mención expresa	Cláusula de exclusion general
Unión Europea		
**Directiva 2017/541 del Parlamento Europeo y del Consejo de 15 de marzo de 2017 relativa a la Lucha Contra el Terrorismo	Solo mención en Preámbulo	Solo mención en Preámbulo
Unión Africana		
Convención para la Prevención y la Lucha Contra el Terrorismo (1999)	Cláusula de exclusión particular	Cláusula de exclusión particular
Protocolo a la Convención para la prevención y la lucha contra el terrorismo (2004)	Ninguna mención expresa	Ninguna mención expresa
Comunidad de Estados Independientes		
Tratado de Cooperación entre los Estados Miembros de la Comunidad de Estados Independientes en la Lucha Contra el Terrorismo (1999)	Ninguna mención expresa	Ninguna mención expresa

*Teniendo en cuenta las apreciaciones realizadas en el presente escrito.
Fuente: elaboración propia.

TRATADOS DE DERECHOS HUMANOS QUE HACEN MENCIÓN EXPRESA AL TERRORISMO

Carta Africana sobre Derechos Humanos y de los Pueblos (1981)	Artículo 33.2
Carta Africana de la Juventud (2006)	Artículo 17

Fuente: elaboración propia.

TRATADOS DE DERECHO INTERNACIONAL HUMANITARIO QUE HACEN MENCIÓN EXPRESA AL TERRORISMO

Cuarto Convenio de Ginebra Relativo a la Protección Debida a las Personas Civiles en Tiempo de Guerra de 1949	Artículo 33
Protocolo Adicional I	Artículo 51.2
Protocolo Adicional II	Artículos 4 y 13.2

Fuente: elaboración propia.

Bibliografía

- BARTELS, Rogier, “Terrorist Groups as Parties to an Armed Conflict, in *Terrorism, Counter-Terrorism and International Humanitarian Law*, 17th Bruges Colloquium 20-21 October 2016
- BOULDEN, Jane, “The United Nations General Assembly and Terrorism” in *Research Handbook on International Law and Terrorism*, Edward Elgar Publishing, Cheltenham, 2020, pp. 493-505
- CARRILLO SALCEDO, Juan Antonio, *Soberanía de los Estados y derechos humanos en derecho internacional contemporáneo*, Tecnos, 2001
- CARTES RODRÍGUEZ, Juan Bautista, *El Sistema Judicial Africano de Protección de los Derechos Humanos. Un análisis de las demandas individuales*, Estudios Aranzadi, Aranzadi, 2023
- CARTES RODRÍGUEZ, Juan Bautista “The Proposed African Criminal Chamber: An Effective Tool To End Impunity On African Soil?”, *Revista Electrónica Cordobesa de Derecho Internacional Público*, 2019, pp. 1-12
- CICR, *Derecho Internacional Humanitario*, Comité Internacional de la Cruz Roja, Ginebra, 2015

- COOMANS, Fons y KAMMINGA, Menno, *Extraterritorial application of human rights treaties*. Antwerp: Intersentia, 2004
- DENNIS, Michael “Application of human rights treaties extraterritorially in times of armed conflict and military occupation”, *American Journal of International Law*, vol. 99, n° 1, 2005, pp. 119-141
- DJEMILA, Carron, *L'acte déclencheur du conflit armé international*, Genève, Schulthess/LGDJ, 2016
- DOSWALD-BECK, Louise, & VITÉ, Sylvain, “International Humanitarian Law and Human Rights Law”, *International Review of the Red Cross*, vol. 33, n° 293, 1993, pp. 94-119
- FERRARO, Tristan “Interaction and Overlap Between Counter-Terrorism Legislation and International Humanitarian Law”, in *Terrorism, Counter-Terrorism and International Humanitarian Law*, 17th Bruges Colloquium 20-21 October 2016
- GAGGIOLI, Gloria, *L'influence mutuelle entre les droits de l'homme et le droit international humanitaire à la lumière du droit à la vie*, Pedone, Paris, 2013
- HEINTZE, Hans-Joachim, “On the Relationship Between Human Rights Law Protection and International Humanitarian Law”, *International Review of the Red Cross*, vol. 86, n° 856, 2004, pp. 789-814
- KRIEGER, Heike, “A conflict of norms: the relationship between Humanitarian Law and Human Rights Law in the ICRC Customary Law Study”, *Journal of Conflict and Security Law*, vol. 11, n° 2, 2006, pp. 265-291
- MEURANT, Jacques, “Droit humanitaire et droits de l'homme: spécificités et convergences”, *International Review of the Red Cross*, vol. 75, n° 800, 1993, pp. 93-98
- MILANOVIC, Marko, *Extraterritorial application of human rights treaties: law, principles, and policy*. Oxford University Press, Oxford, 2011
- HATHAWAY, Oona et. al., “Which law governs during armed conflict the relationship between International Humanitarian Law and Human Rights Law”, *Minnesota Law Review*, vol. 96, n° 6, 2012, pp. 1883-1943
- PICTET, Jean, *Commentary of the Geneva Convention Relative to the Protection of Civilian Persons in Time of War*, International Committee of the Red Cross, 1958, pp. 225-226
- PROVOST, Rene, *International Human Rights and Humanitarian Law*, Cambridge University Press, Cambridge, 2002

- SALMÓN, Elisabeth, *Introducción al Derecho Internacional Humanitario*, CICR, 2004
- SANDOZ, Yves, SWINARSKI, Christophe y ZIMMERMANN, Bruno, *Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949*, Martinus Nijhoff Publishers, International Committee of the Red Cross, Geneva, 1987
- SASSÒLI, Marco, “Legal Qualification of the Fight Against Terrorism”, in *Terrorism, Counter-Terrorism and International Humanitarian Law*, 17th Bruges Colloquium 20-21 October 2016
- ÚBEDA-PORTUGUÉS, José Escribano “Nuevos avances y retos en la lucha contra el terrorismo”, *Revista Electrónica de Estudios Internacionales*, vol. 17, 2009, pp. 1-15

A governança global do terrorismo: o papel do Conselho de Segurança das Nações Unidas

The Global Governance of Terrorism: The Role of the Nations Security Council

Maria do Céu Pinto Arena

Resumo: Desde os acontecimentos de 11 de setembro de 2001, o terrorismo tornou-se uma das mais importantes ameaças à segurança internacional. Este artigo tem por objetivo apresentar uma panorâmica introdutória do papel do Conselho de Segurança (CSNU) na luta contra o terrorismo. O argumento central deste artigo assenta na ideia de que, após o 11 de setembro, o CSNU passou a desempenhar um papel decisivo na governança global do terrorismo, tornando-se o principal órgão de coordenação multilateral e a força motriz da luta contra o terrorismo. Este artigo aborda o seu papel normativo neste domínio, as preocupações com as disposições na área do contraterrorismo relativamente às liberdades civis, as estruturas de apoio e o papel do CSNU na «arquitetura do contra-terrorismo».

Palavras-chave: Arquitetura de contra-terrorismo; Conselho de Segurança das Nações Unidas; Resoluções normativas; terrorismo.

Abstract: Since the events of September 11, 2001, terrorism has become one of the most significant threats to international security. This article aims to provide an introductory overview of the role of the United Nations Security Council (UNSC) in the fight against terrorism. The central argument of this article is based on the idea that, after September 11, the UNSC began to play a decisive role in the global governance of terrorism, establishing itself as the main multilateral coordination body and the driving force behind counterterrorism efforts. This article examines its normative role in this area, concerns regarding counterterrorism provisions and civil liberties, support structures, and the UNSC's role within the “counterterrorism architecture.”

Keywords: counterterrorism architecture; normative resolutions; terrorism; United Nations Security Council.

Sumário: 1.Introdução; 2. O papel do Conselho de Segurança da ONU na luta contra o terrorismo; 3. Conclusão.

Lista de abreviaturas: ADMs – Armas de Destruição Massiva; AGNU – Assembleia Geral das Nações Unidas; CCT – Comité Contraterrorismo; CSNU – Conselho de Segurança das Nações Unidas; EIIS – Estado Islâmico do Iraque e da Síria; GTCF – Fórum Mundial de Luta contra o Terrorismo; ONU – Organização das Nações Unidas; UNODC – Gabinete das Nações Unidas contra a Droga e o Crime.

1. Introdução

Passou já mais de meio século desde que a Assembleia Geral (AGNU) da Organização das Nações Unidas (ONU) negociou a sua primeira convenção antiterrorista (sobre crimes cometidos a bordo de aeronaves) e cerca de 25 anos desde que o CSNU impôs sanções contra a Líbia devido ao patrocínio de atos de terrorismo por parte daquele Estado. Contudo, foi só após os atentados terroristas de 11 de setembro de 2001 que a ONU aprovou uma profusão de medidas da ONU para enfrentar a ameaça terrorista. Em 2006, a AGNU adotou uma Estratégia Global contra o Terrorismo¹. Contudo, mesmo após o 11 de setembro, as propostas para envolver a ONU na luta contraterrorismo foram recebidas com uma grande dose de ceticismo².

Nestes anos, a ONU criou uma verdadeira arquitetura de contraterrorismo³. Esta comunicação tenta fornecer uma avaliação do impacto e das limitações dos esforços globais de combate ao terrorismo por parte do CSNU. O trabalho antiterrorista da ONU pode ser organizado em três níveis:

¹ Revista em 2021.

² ALEXANDER MARSCHIK, «The Security Council's Role: Problems and Prospects in the Fight against Terrorism», in *International Cooperation in Counter-terrorism. The United Nations and Regional Organizations in the Fight Against Terrorism*, Giuseppe Nesi (ed.), Ashgate Publishing, Hampshire/Burlington, 2006, p. 60.

³ Ver UNITED NATIONS, OFFICE OF COUNTER-TERRORISM, *Main Bodies*, acessível em <https://www.un.org/en/about-us/main-bodies> (consulta feita em 16 de outubro de 2023).

1. um papel normativo que inclui: a) o desenvolvimento e promoção de uma Estratégia contra o Terrorismo e esforços para combater a violência e extremismo; b) a aprovação de um conjunto de convenções internacionais; c) a adoção de resoluções abrangentes do CSNU que impõem obrigações no combate ao terrorismo;
2. desenvolver as capacidades dos Estados para combaterem o fenómeno;
3. a imposição de sanções pelo CSNU desde a década de 1990 contra os patrocinadores estatais do terrorismo e centenas de indivíduos e entidades afiliadas à al-Qaeda e ao Estado Islâmico do Iraque e da Síria⁴.

2. O papel do Conselho de Segurança da ONU na luta contra o terrorismo

O papel de maior importância na instituição de um regime jurídico reforçado contra o terrorismo coube ao CSNU, ator que rapidamente consolidou o seu papel liderante no contraterrorismo. O primeiro destaque vai para a Resolução 1373 (28 de setembro de 2001)⁵. Esta cria um novo regime⁶, obrigando os Estados a adotarem uma série de medidas de criminalização e supressão de atividades terroristas, bem como a proibição de apoio e financiamento de atentados e organizações terroristas⁷. O segundo regime é a

⁴ Na sequência da Resolução 2253 de 17 de dezembro de 2015, o Comité de Sanções do CSNU contra o Talibãs e al-Qaeda, também chamado Comité 1267, atualizou a sua Lista de Sanções, incluindo contra o grupo terrorista, Estado Islâmico do Iraque e da Síria (EIIS): UNSC, *Resolution 2253*, S/RES/2253, 2015, acessível em <https://documents-dds-ny.un.org/doc/UNDOC/GEN/N15/437/45/PDF/N1543745.pdf?OpenElement> (consulta feita em 17 de outubro de 2023).

⁵ UNSC, *Resolution 1373*, S/RES/1373, 2001, acessível em https://www.unodc.org/pdf/crime/terrorism/res_1373_english.pdf (consulta feita em 17 de outubro de 2023).

⁶ MARSCHIK, *The Security Council's Role*, cit., p. 70.

⁷ *Id.* Ver também JAYANTHA DHANAPALA, «The United Nations' Response to 9/11», *Terrorism and Political Violence*, vol. 17, nº 1, 2005, p. 18; HILDE HAALAND KRAMER e STEVE A. YETIV, «The UN Security Council's Response to Terrorism: Before and After September 11, 2001», *Political Science Quarterly*, vol. 122, nº 3, 2007, p. 414; EDWARD C. LUCK, «Tackling Terrorism», in *The UN Security Council: From the Cold War to the 21st Century*, David Malone (ed.), Lynne Rienner Publishers, Boulder, CO/Londres, 2004, p. 96; CHANTAL DE JONGE OUDRAAT, «The United Nations and the campaign against terrorism», *Disarmament Forum*, nº 1, 2004, p. 69.

Resolução 1267 (15 de outubro de 1999)⁸, subsequentemente expandida, e que cria regimes de sanções contra os Talibás, al-Qaeda e, mais recentemente, o EIIS. Assenta numa série de sanções (embargo de armas, proibição de viajar, congelamento de fundos) contra indivíduos e entidades enumerados numa extensa lista. A sua implementação é monitorizada pelo Comité 1267.

Esta Resolução desbravou terreno novo ao invocar, pela primeira vez, os poderes do Capítulo VII da Carta da ONU para dar orientações imperativas aos Estados-Membros num contexto genérico, não diretamente relacionado a disciplinar qualquer Estado individualmente ou ator⁹. Ao referir-se ao Capítulo VII da Carta da ONU, o CSNU abre possibilidade de tomar medidas contra Estados que não cumpram esta Resolução, através de sanções ou medidas coercivas, incluindo o uso da força¹⁰. Recorde-se que no dia 12 de setembro de 2001, o CSNU tinha aprovado a Resolução 1368, reconhecendo «o direito natural de legítima defesa individual ou coletiva de acordo com a Carta» e considerando os ataques, «tal como qualquer ato de terrorismo internacional, uma ameaça à paz e segurança internacional»¹¹. Esta associação – terrorismo internacional e direito de legítima defesa – levantava, contudo, algumas questões importantes.

«Ao invocar o direito de legítima defesa de um Estado e, assim, legitimar a utilização unilateral da força contra ataques terroristas, o CSNU abriu um importante precedente que põe em risco a proibição geral de uso da força, consagrada na Carta da ONU. De facto, os Estados Unidos pareceram considerar a Resolução 1368 como um cheque em branco. A China e a Rússia (...) foram

⁸ UNSC, *Resolution 1267*, S/RES/1267, 1999, acessível em <https://documents-dds-ny.un.org/doc/UNDOC/GEN/N99/300/44/PDF/N9930044.pdf?OpenElement> (consulta feita em 17 de outubro de 2023).

⁹ Desta forma, as disposições da Convenção para a Supressão do Financiamento do Terrorismo (1999), cujo conteúdo consta genericamente na Resolução, deixaram de ser opcionais para serem juridicamente vinculativas.

¹⁰ Jeffrey Laurenti observa «[n]unca antes o Conselho reconheceu a autodefesa militar como aplicável contra ações cometidas por atores não estatais», em JOE SILLS, «The United Nations and the Formation of Global Norms», in *The United Nations: Confronting the Challenges of Global Society*, JEAN E. KRASNO (ed.), Lynne Rienner Publishers, Boulder, CO/Londres, 2004, p. 69.

¹¹ UNSC, *Resolution 1368*, S/RES/1368, 2001, acessível em <https://documents-dds-ny.un.org/doc/UNDOC/GEN/N01/533/82/PDF/N0153382.pdf?OpenElement> (consulta feita em 17 de outubro de 2023).

céleres no apoio à posição dos EUA: Pequim acreditava que iria ajudar a legitimar a supressão de grupos opositores em Xinjiang, ao passo que a Rússia a encarava como um precedente útil na sua luta contra os rebeldes chechenos. De facto, em setembro de 2002, Moscovo invocou a Resolução 1368 para justificar possíveis ataques militares contra rebeldes chechenos a operar na Geórgia – com ou sem autorização do Governo georgiano»¹²

Estas resoluções são apenas o início de uma intensa atividade legislativa com a aprovação, até hoje, de mais de vinte resoluções, e transformando o CSNU naquilo que James Cockayne ou Stefan Talmon designam como uma «uma legislatura mundial» ao afirmarem que «foi uma maneira nova e radical de impor normas contra atos criminais à sociedade internacional, transformando o Conselho de Segurança numa espécie de “legislatura mundial”»¹³.

Apesar de algum sucesso na promoção de padrões internacionais na luta contra o terrorismo, há quem conteste as competências normativas/legislativas do CSNU que estabelecem uma série de metas legislativas para os Estados alcançarem através da promulgação de legislação nacional. Como afirmou Derek Bowett, o CSNU é um órgão executivo, não legislativo¹⁴. Desde o fim da Guerra Fria, no entanto, o CSNU expandiu os seus poderes devido a uma ampla interpretação do conceito de paz e segurança, bem como outorgando-se vastas funções executivas, quase-judiciais e legislativas, culminando na adoção de resoluções normativas, numa situação qualificada como de «hegemonia legalizada»¹⁵. Tal inclui a elaboração de leis abstratas, como quando o CSNU considerou o terrorismo, em abstrato, como uma ameaça contra a paz e a segurança e impôs obrigações legais aos Estados de

¹² CHANTAL DE JONGE OUDRAAT, «Combating Terrorism», *The Washington Quarterly*, vol. 24, nº 4, 2003, p. 168.

¹³ JAMES COCKAYNE, «Counterterrorism and Transnational Crime», in *The Oxford Handbook of International Organizations*, Jacob Katz Cogan, Ian Hurd e Ian Johnstone (eds.), Oxford University Press, Oxford, 2016, p. 219; STEFAN TALMON, «The Security Council as World Legislature», *American Journal of International Law*, vol. 99, nº 1, 2005, pp. 175-193.

¹⁴ DEREK BOWETT, «The Impact of Security Council Decisions on Dispute Settlement Procedures», *European Journal of International Law*, 1994, vol. 5, nº 1, p. 93.

¹⁵ MUNIR AKRAM e SEYYED HAIDER SHAH, «The Legislative Powers of the United Nations Security Council», in *Towards World Constitutionalism: Issues in the Legal Ordering of the World Community*, Ronald St. John Macdonald e Douglas M. Johnston (eds.), Martinus Nijhoff Publishers, Leiden/Boston, 2005, p. 438.

adotar medidas específicas, normalmente prescritas por tratados internacionais. No caso da Resolução 1373, trata-se de uma competência quase legislativa¹⁶, equivalente à capacidade negocial dos Estados, num sistema equivalente à negociação de tratados internacionais¹⁷.

A autoridade do CSNU para exercer tal função foi questionada e a sua legitimidade foi posta em causa já que aquelas resoluções normativas foram iniciadas e adotadas indevidamente sob a influência de um Membro Permanente, os EUA¹⁸. As resoluções normativas do CSNU enfrentaram sérios desafios na fase de implementação e houve diversos processos perante tribunais nacionais e regionais que têm desafiado diretamente as resoluções normativas ou questionado a sua aplicabilidade. Em 2004, o CSNU ampliou ainda mais o seu programa contraterrorismo de forma a implementar a Resolução 1540 (28 de abril de 2004)¹⁹, a qual visa impedir os Estados de apoiarem os esforços de «agentes não-estatais» para desenvolverem ou adquirirem, armas nucleares, químicas ou biológicas – reflexo da crescente preocupação do CSNU com a associação entre terrorismo internacional e a proliferação de Armas de Destruição Massiva (ADMs).

O CSNU está sob pressão contínua para continuar a rever a sua prática ou potencialmente enfrentar desafios adicionais perante tribunais nacionais, regionais e até internacionais que podem anular ou revogar as medidas de

¹⁶ PAUL SZAZ, «The Security Council Starts Legislating», *American Journal of International Law*, vol. 96, nº 4, 2002, pp. 901-905.

¹⁷ ILIAS BANTEKAS, «The International Law of Terrorist Financing», *The American Journal of International Law*, vol. 97, nº 2, 2003, p. 315.

¹⁸ SAEID MIRZAEI YENGEJEH, *Law-Making by the Security Council in Areas of Counter-Terrorism and Non-Proliferation of Weapons of Mass-Destruction*, Thesis Submitted for the Degree of Doctorate in Philosophy in Law of the University of Ottawa, Faculty of Common Law, Universidade de Ottawa, 2016; JOSÉ E. ALVAREZ, «The UN's 'War' on Terrorism», *International Journal of Legal Information*, vol. 31, nº 2, 2003, p. 238, 241; MATTHEW HAPPOLD, «Security Council Resolution 1373 and the Constitution of the United Nations», *Leiden Journal of International Law*, vol. 16, nº 3, 2003, p. 593, 596; NICO KRISCH, «The Rise and Fall of Collective Security: Terrorism, US Hegemony, and the Plight of the Security Council», in *Terrorism as a Challenge for National and International Law: Security Versus Liberty?*, Christian Walter, Silja Vöneky, Volker Röben e Frank Schorkopf (eds.), Springer, Berlim/Nova Iorque, 2003, p. 879, 883.

¹⁹ UNSC, *Resolution 1540*, S/RES/1540, 2004, acessível em [https://daccess-ods.un.org/access.nsf/Get?OpenAgent&DS=S/RES/1540\(2004\)&Lang=E](https://daccess-ods.un.org/access.nsf/Get?OpenAgent&DS=S/RES/1540(2004)&Lang=E) (consulta feita em 17 de outubro de 2023).

implementação relevantes. A abordagem dominante entre 2001 e 2004 revelou ter efeitos controversos e também contraproducentes: o reforço legislativo na área do contraterrorismo, impulsionada pela ONU, fez com que a regulamentação nacional fosse elaborada em detrimento das liberdades civis. De facto, vários governos – autoritários e democráticos – instrumentalizaram o ímpeto antiterrorista, vivido internacionalmente após o 11 de setembro para eliminar os seus opositores internos. Ora, esses efeitos perversos começaram a ser reconhecidos pela ONU a partir de 2005. Observa-se, nesta fase, duas vias institucionais fulcrais no seio das quais foi reavivada a preocupação com os direitos e liberdades fundamentais dos cidadãos: a adoção da Estratégia Global Contra o Terrorismo (2006); o envolvimento do próprio Conselho dos Direitos Humanos na questão antiterrorista, nomeadamente com a criação do cargo de Relator Especial para a Promoção e Proteção dos Direitos Humanos e Liberdades Fundamentais no âmbito do Combate ao Terrorismo.

Embora a ausência de uma convenção abrangente não represente uma lacuna grave na lei (quase todas as formas de terrorismo são proibidas pelas várias organizações setoriais, convenções ou pelo direito penal internacional), tal não impediu a ação robusta de combate ao terrorismo da ONU no pós-11 de setembro. Esta prejudica decerto a autoridade moral da organização, inibindo-a de enviar uma mensagem inequívoca de que o terrorismo nunca é uma tática aceitável. Mais importante ainda é que o fato de não haver uma definição consensual de terrorismo, cria sérios problemas de Direitos Humanos, pois tal permite que alguns governos justifiquem o julgamento de divergências políticas legítimas como forma de combater o terrorismo exigido por mandatos de longo alcance do CSNU.

A Resolução 1373 pode ser facilmente usada de forma indevida para visar indivíduos ou grupos minoritários por razões políticas²⁰. Contudo, é de sublinhar que os comités, criados no âmbito dos regimes acima referidos, se abstiveram de ir para além do paradigma interestatal, isto é, da adoção de medidas contra indivíduos ou outras entidades privadas. Além disso, embora o Comité Contraterrorismo (*CCT/Counter-Terrorism Committee*) tem funcionado predominantemente como órgão de assistência técnica que depende fortemente da cooperação dos Estados. O Comité contribui

²⁰ MARSCHIK, *The Security Council's Role*, cit., pp. 72-73.

para o reforço das capacidades para apoiar os esforços dos Estados-Membros no sentido de tomarem medidas práticas para prevenir e combater o terrorismo através de uma vasta gama de atividades, projetos e programas. O mesmo se aplica ao Comité de Não-Proliferação. Em essência, portanto, pode-se argumentar que a implementação dos regimes previstos na Resolução 1373 e na Resolução 1540, combinada com a natureza predominantemente voluntária dos órgãos de monitorização estabelecidos por essas resoluções, reduziram o seu impacto: o CTC não dispõe de capacidades executivas, isto é, de mecanismos efetivos para forçar os Estados a implementarem as medidas obrigatórias definidas na Resolução 1373.

O CCT e a Direção Executiva do Comité destinada a assistir o CCT na implementação do seu mandato²¹ têm-se debatido com alguns problemas e limitações no decurso da sua ação. Primeiro, os vários Estados entendiam as disposições da Resolução 1373 de forma diversa. Segundo, alguns Estados apenas tomavam medidas para suprimir as atividades terroristas nos seus territórios, mostrando-se permissivos com atos empreendidos no estrangeiro pelos seus cidadãos. Terceiro, as informações fornecidas ao CCT eram, de uma forma geral, muito vagas, centrando-se essencialmente em aspetos jurídicos. Finalmente, apenas um número reduzido de Estados mostrou recetividade para aceitar assistência técnica, apesar de muitos experimentarem um défice de capacidades legislativas e administrativas na implementação das medidas exigidas pelo CSNU²². Com o passar do tempo, também se acentuou a dita *reporting fatigue*.

Existem outras questões importantes relacionadas com a atividade do CCT e da Direção Executiva do Comité destinada a assistir o CCT na implementação do seu mandato²³. Primeiro, existe o risco de duplicação de funções com outros organismos ou agências especializadas da Organização – particularmente, o Gabinete das Nações Unidas contra a Droga e o Crime (UNODC) – já mandatados para tratar aspetos relacionados com o fenómeno do terrorismo internacional²⁴. Segundo, o CCT dispõe de recursos – humanos e financeiros – muito limitados.

²¹ UNSC, *Resolution 1535*, S/RES/1535, 2004, acessível em <https://documents-dds-ny.un.org/doc/UNDOC/GEN/N04/286/41/PDF/N0428641.pdf?OpenElement> (consulta feita em 17 de outubro de 2023).

²² OUDRAAT, «Combating Terrorism», cit., p. 170.

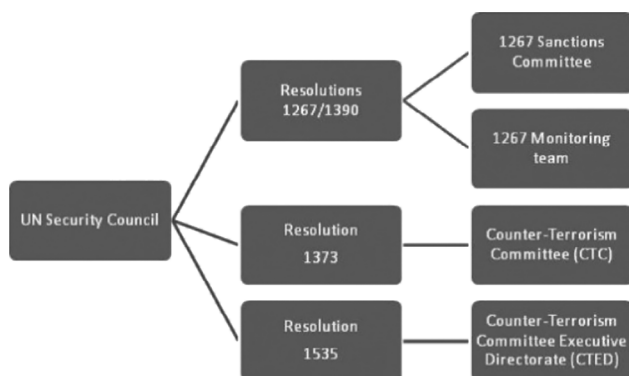
²³ UNSC, *Resolution 1535*, cit.

²⁴ DHANAPALA, «The United Nations' Response to 9/11», cit., p. 19.

A ação do CSNU na condenação e combate ao terrorismo internacional foi complementada pelos esforços do Secretário-Geral das Nações Unidas e pela AGNU. Preocupada com a o exclusivo controle do CSNU sobre a agenda de antiterrorismo da ONU, o Secretário-Geral das Nações Unidas e a AGNU tentaram afirmar seu próprio papel nesta área. No entanto, esta multiplicação de obrigações causou confusão e discórdia, levando muitos Estados-Membros a apelar a uma maior coordenação de todas as abordagens da ONU para cumprir as resoluções do CSNU e da AGNU sobre o terrorismo.

É nesse sentido que, em junho de 2017, o Secretário-Geral das Nações Unidas, António Guterres, tentou melhorar substancialmente a coordenação e a coerência dos esforços de luta contra o terrorismo das Nações Unidas. Em fevereiro de 2018, o Escritório passou a ser presidido por um Subsecretário-Geral do Gabinete de Contraterrorismo, Vladimir Voronkov²⁵.

Figura 1. A arquitetura de segurança da ONU



Fonte: Charity Security Network²⁶

²⁵ O Pacto Global de Combate ao Terrorismo é um acordo entre o Secretário-Geral das Nações Unidas e trinta e seis entidades da ONU, a Organização Internacional de Polícia Criminal (INTERPOL) e a Organização Mundial das Alfândegas no âmbito da reforma do Secretário-Geral das Nações Unidas, António Guterres, da arquitetura antiterrorista da ONU. É a maior estrutura de coordenação nas Nações Unidas nos quatro pilares de trabalho da organização: paz e segurança, desenvolvimento sustentável, Direitos Humanos e assuntos humanitários.

²⁶ CHARITY SECURITY NETWORK, *UN Counterterrorism Framework: Key Programs and Tools*, acessível em https://charityandsecurity.org/analysis/un_counterterrorism_framework_key_programs_and_tools/ (consulta feita em 17 de outubro de 2023).

Não admira, por isso que os EUA tenham, em 2011, sob o Presidência Obama, criado o Fórum Mundial de Luta contra o Terrorismo (*Global Counterterrorism Forum – GCTF*), uma plataforma «orientada para a ação» fora do quadro da ONU. Esta iniciativa pretende promover uma cooperação multilateral mais eficaz no âmbito do contraterrorismo, em particular no que diz respeito à capacitação dos Estados. O GCTF trabalha em estreita colaboração com os organismos da ONU e dá prioridade ao reforço das capacidades civis em domínios como o Estado de Direito, a gestão das fronteiras e a prevenção e luta contra o extremismo violento. Um dos principais objetivos do Fórum é ainda catalisar a implementação da Estratégia Global de Luta contra o Terrorismo das Nações Unidas, revista em junho de 2021²⁷, e do Quadro de Combate ao Terrorismo das Nações Unidas em termos mais gerais, incluindo, por exemplo, o Plano de Ação do Secretário-Geral das Nações Unidas para Prevenir o Extremismo Violento apresentado à Assembleia Geral das Nações Unidas em janeiro de 2016²⁸. Relativamente à Resolução 1540, o GCTF, da mesma forma que a administração Obama, concluiu que, enquanto a Resolução forneceu uma estrutura normativa útil, do ponto de vista operacional, a ONU é muito lenta e burocrática. Tal levou Washington a estabelecer uma nova iniciativa fora do quadro da ONU: as Cimeiras de Segurança Nuclear, destinadas a melhorar a cooperação internacional para prevenir o tráfico nuclear e terrorismo.

3. Conclusão

Na sequência dos atentados de 11 de setembro, o CSNU desenvolveu um papel central no combate ao terrorismo. O CSNU tornou-se o «principal órgão de coordenação multilateral e a força dinamizadora no campo do contraterrorismo»²⁹. A Resolução 1368 abriu caminho à militarização das

²⁷ UNITED NATIONS GENERAL ASSEMBLY (UNGA) *Resolution adopted by the General Assembly on 30 June 2021, A/RES/75/291*, 2021, acessível em <https://documents-dds-ny.un.org/doc/UNDOC/GEN/N21/175/70/PDF/N2117570.pdf?OpenElement> (consulta feita em 2 de novembro de 2023).

²⁸ UNGA, *Plan of Action to Prevent Violent Extremism*, A/70/674, 2015, acessível em <https://documents-dds-ny.un.org/doc/UNDOC/GEN/N15/456/22/PDF/N1545622.pdf?OpenElement> (consulta feita em 2 de novembro de 2023).

²⁹ MARSCHIK, *The Security Council's Role*, cit., p. 69.

respostas ao terrorismo internacional e a Resolução 1373 globalizou o combate ao terrorismo. A este nível, trata-se de um processo eminentemente político e menos de um processo tecnocrático. No entanto, não deixa de ser verdade que o contraterrorismo motivou um reforço do multilateralismo, pois o ímpeto para a cooperação deu origem a uma rede de instituições, iniciativas e mecanismos multilaterais. Não obstante um esforço por parte do CSNU de construção de um regime internacional de combate ao terrorismo, baseado nos princípios de cooperação e ação coletiva, a verdade é que esta ação tem sido minada pelas atitudes dos principais *players* na cena internacional – os Estados. Evidenciam-se por isso divergências e um fraco consenso entre os Estados-Membros da ONU relativa às prioridades deste combate.

Os desafios são muitos, mas é possível elencar alguns: existem problemas técnicos e práticos na implementação das normas; nem tudo se explica pela falta de vontade política. A capacidade de implementar as resoluções é por vezes limitada. A ONU e o CCT nem sempre conseguem ajudar os Estados a fortalecer a sua capacidade na prevenção e combate ao terrorismo. É ainda necessário continuar a assegurar o respeito pelos Direitos Humanos e o primado da Lei no combate ao terrorismo.

A nível da ONU, é necessário assegurar a coordenação e a coerência globais nos esforços de contraterrorismo desenvolvidos no âmbito do sistema da ONU. A atual abordagem é fragmentária, dadas as numerosas entidades dentro do sistema das Nações Unidas com mandatos antiterrorismo. Seria necessário reestruturar a atual «arquitetura contraterrorista» em favor de uma abordagem estrategicamente coesa, holística e coordenada para derrotar o extremismo.

Apesar destas limitações, a ONU tem efetivamente se constituído como um caminho útil para o estabelecimento de um quadro normativo e cooperativo global na resposta contraterrorista, estando bem posicionada para fortalecer a colaboração aos níveis regional, nacional e internacional. Quando analisada ao longo do tempo, a capacidade política e institucional das Nações Unidas tem evoluído de forma positiva, pelo que os desafios descritos acima demonstram um progresso que é gradual.

O Papel da Primeira Comissão da Assembleia Geral das Nações Unidas no Desenvolvimento de um Ciberespaço Estável e Seguro. Perspetivas Político-Militares sobre a Resolução «Desenvolvimentos no Campo da Informação e Telecomunicações no Contexto da Segurança Internacional»

The Role of the United Nations General Assembly First Committee in Developing a Stable and Secure Cyberspace. Political and Military Perspectives on the Resolution “Developments in the Field of Information and Telecommunications in the Context of International Security”

Maria Francisca Saraiva

Resumo: A aprovação da Resolução «Desenvolvimentos no Campo da Informação e Telecomunicações no Contexto da Segurança Internacional» em 1999 na Primeira Comissão da Assembleia Geral das Nações Unidas, dedicada ao desarmamento e segurança internacional, colocou na agenda desta Comissão a promoção do desenvolvimento de um ciberespaço estável, pacífico e seguro. Neste texto, mostramos que a regulação do ciberespaço no quadro da Primeira Comissão é para os Estados Unidos, a Rússia e a China uma arena ideológica e de projecção de poder centrada

Abstract: The approval of the Resolution “Developments in the Field of Information and Telecommunications in the Context of International Security” in 1999 in the United Nations General Assembly First Committee, dedicated to disarmament and international security, included in the agenda of this Commission the promotion of the development of a stable, peaceful and secure cyberspace. In this text, we show that the regulation of cyberspace within the framework of this Commission is, for the United States, Russia, and China an ideological and power projection arena centered on defining

na definição do regime de acesso e uso do ciberespaço a respeito de várias matérias político-estratégicas de grande relevância e um novo campo de batalha em torno da possibilidade de travar guerras no ciberespaço ou a partir do ciberespaço. Sugere-se que o estudo das dinâmicas políticas na Primeira Comissão sobre este tema tem uma relevância que ultrapassa significativamente o mandato da Primeira Comissão em relação à regulação ao ciberespaço numa perspetiva de segurança internacional.

Palavras-chave: Assembleia Geral – Primeira Comissão; Ciberagressão; Cibercrime; Ciberterrorismo; Nações Unidas.

the regime of access and use of cyberspace concerning various political-strategic issues of great relevance. and a new battlefield around the possibility of waging wars in or from cyberspace. It is suggested that the study of political dynamics in the First Commission on this topic has a relevance that significantly goes beyond the mandate of the First Commission concerning the regulation of cyberspace from an international security perspective.

Keywords: cyberaggression; cybercrime; cyberterrorism; General Assembly – First Committee; United Nations.

Sumário: 1. Introdução; 2. O Papel da Resolução “Desenvolvimentos no Campo da Informação e Telecomunicações no Contexto da Segurança Internacional” nas Estratégias Russa e Chinesa; 3. Os Grupo de Peritos Governamentais; 3.1. Primeiro Grupo de Peritos Governamentais (2004/2005); 3.2. Segundo Grupo de Peritos Governamentais (2009/2010); 3.3. Terceiro Grupo de Peritos Governamentais (2012/2013); 3.4. Quarto Grupo de Peritos Governamentais (2014/2015); 3.5. Quinto Grupo de Peritos Governamentais (2016/2017); 3.6. Sexto Grupo de Peritos Governamentais (2019/2021); 4. Os OEWG; 4.1. Primeiro Grupo de Trabalho Aberto (2018-2021); 4.2. Segundo OEWG (2021-2025); 5. Manobras Diplomáticas Recentes; 6. Conclusões.

1. Introdução

O espaço cibernético afeta os mais variados aspetos da vida quotidiana. Em particular, a relação do homem com este novo contexto permitiu a emergência acelerada de um novo domínio de poder nas relações internacionais onde atuam atores de diversa natureza, nomeadamente Estados, organizações criminosas e organizações terroristas. Por causa da rapidez destas mudanças

é muito importante definir o quanto antes um regime internacional de acesso e uso do ciberespaço que promova um ciberespaço estável, pacífico e seguro.

A complexidade desta nova realidade levou à necessidade de criar vários fóruns de negociação para discutir os assuntos relacionados com a cibersegurança, a começar pelas Nações Unidas (NU). Mas o tema figura ainda na agenda de várias outras organizações internacionais e fóruns de discussão que se preocupam com o problema da (in)segurança do espaço virtual.

Este texto procura entender o papel da Primeira Comissão da Assembleia Geral das Nações Unidas (AGNU) no enquadramento dos problemas político-militares do ciberespaço a partir da resolução «Desenvolvimentos no Campo da Informação e Telecomunicações no Contexto da Segurança Internacional» (A/RES/53/70, de 4 de janeiro de 1999).

A Primeira Comissão da AGNU é um órgão de natureza intergovernamental que na ONU recebeu mandato para discutir a dimensão político-militar do ciberespaço, com o objetivo de estabelecer um conjunto de regras que permitam uma utilização do ciberespaço mais segura, previsível e estável. Entre outros aspetos, a Comissão está mandatada para avaliar a possibilidade de os Estados travarem guerras no ciberespaço ou a partir do ciberespaço¹.

A ambição da ONU no desempenho de um papel central na governação global de ciberespaço também é visível no trabalho de outras Comissões principais da AGNU como é o caso da Segunda Comissão, que se dedica à cooperação internacional de natureza económico-financeira e ao desenvolvimento sustentável procurando a regulação internacional do espaço ciber através de uma resolução sobre a promoção de uma «cultura global de cibersegurança» e a proteção das infraestruturas críticas². Também de referir o acompanhamento dado pela Terceira Comissão (assuntos sociais, humanitários e culturais), que trata de Direitos Humanos (DH), Direito Internacional Humanitário (DIH), justiça criminal e prevenção do crime, incluindo terrorismo)³ e pelo Conselho Económico e Social, dois fóruns de negociação

¹ É uma das seis Comissões principais da Assembleia Geral e é aberta a todos os cento e noventa e três Estados que pertencem à organização.

² UNITED NATIONS, *The United Nations, Cyberspace and International Peace and Security Responding to Complexity in the 21st Century*, New York, UNIDIR Resources, 2017, p.21.

que têm procurado vincular os DH à questão dos abusos associados ao uso das Tecnologias de Informação e Comunicação (TIC), assim como se têm ocupado da dimensão económica da cibersegurança⁴. Finalmente, a Sexta Comissão da AGNU (assuntos jurídicos) tem capacidade de se vir a ocupar das questões do ciberterrorismo. De momento, não é essa a situação pelo fato de nenhuma das convenções onusianas que regulam o terrorismo incluírem a dimensão do ciberterrorismo, o que tem retirado a esta Comissão a capacidade de contribuir de forma ativa para a regulação do ambiente ciber⁵. Assim, dado que a Segunda e a Terceira Comissões tendem a dar resposta a ameaças transnacionais como o terrorismo ou os atos criminosos perpetrados no ciberespaço, a Primeira Comissão tem assumido como principal responsabilidade lidar com as questões político-estratégicas mais diretamente relacionadas com o problema da militarização do ciberespaço. Esta divisão de tarefas não é, contudo, perfeita: a Primeira Comissão tem vindo a refletir sobre outras dimensões relevantes do uso responsável do ciberespaço pelos Estados temas que, como acima referido, cruzam com a agenda das Segunda e Terceira Comissões.

Recentemente, o assunto da segurança cibernética passou a figurar também na agenda do Conselho de Segurança das Nações Unidas (CSNU). Reconhecendo a premência da problemática na ótica da segurança, o CSNU organizou, em 2021, um primeiro debate de alto nível sobre o crescente uso malicioso das tecnologias digitais (S/2021/621, de 29 de junho de 2021). Nesta sessão foi discutida a questão de o ciberespaço estar a tornar-se cada vez mais militarizado, politizado, inseguro e ideologizado. Nesta ocasião os Estados voltaram a esgrimir argumentos contraditórios sobre a possibilidade de ciberataques, cibercrimes e políticas de cibervigilância colocarem em causa a paz e a segurança internacionais. Estes argumentos já são bem conhecidos da Primeira Comissão da AGNU onde ao longo dos anos os

³ UNITED NATIONS, *The United Nations, Cyberspace*, cit., p.13.

⁴ TIM MAURER, *Cyber Norm Emergence at the UN*, Belfer Center Discussion Paper 2011-11, Cambridge, Harvard Kennedy School, 2011, p.36.

⁵ No seio da Terceira Comissão, foi decidido negociar uma Convenção sobre Cibercrime (*Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes*). Os trabalhos estão em curso, não se sabendo, à data de hoje, se irá contemplar a questão do ciberterrorismo.

Estados que participam nos seus trabalhos têm apresentado repetidamente as suas discordâncias relativamente ao impacto destas problemáticas no sistema internacional.

2. O Papel da Resolução «Desenvolvimentos no Campo da Informação e Telecomunicações no Contexto da Segurança Internacional» nas Estratégias Russa e Chinesa

A Rússia foi a grande impulsionadora do debate sobre o uso responsável do ciberespaço pelos Estados com a introdução na agenda na Primeira Comissão da AGNU (Comissão de Desarmamento e Segurança Internacional) da Resolução «Desenvolvimentos no Campo da Informação e Telecomunicações no Contexto da Segurança Internacional» (A/RES/53/70, de 4 de janeiro de 1999), continuando nos dias de hoje a liderar os esforços de regulação da segurança cibernética.

Sobre esta temática vale a pena lembrar que nos finais do século XX, ainda como União Soviética, a literatura militar já assinalava que se encontraria em curso nos Estados Unidos uma revolução tecnológica militar que acentuava o fosso tecnológico entre as duas superpotências⁶. Esta preocupação com os desenvolvimentos tecnológicos americanos vinha, aliás, da década anterior, sendo relevante aqui referir episódios de espionagem russa a propósito da Iniciativa de Defesa Estratégica (IDE ou SDI no original, mais conhecida por «Guerra das Estrelas»). Anunciada por Reagan em 1983, a IDE era um programa militar do governo norte-americano de grande envergadura que propunha que a indústria nacional desenvolvesse as capacidades necessárias ao estabelecimento de um sistema de defesa antimíssil de âmbito nacional. Mais tarde, em 1991, a Guerra do Golfo mostrou que algo novo estava a acontecer ao nível da capacidade militar convencional nos Estados Unidos: com o uso das TIC⁷ o ciberespaço e o espaço exterior assumiam-se como novos teatros de operações onde a supremacia militar americana permitiria

⁶ ANTÓNIO JOSÉ TELO, «Reflexões sobre a Revolução Militar em Curso», *Nação e Defesa*, nº 103, 2002, pp. 211-249, na p.221.

⁷ MYRIAM DUNN CAVELTY, «Cyber-Threats», in *The Routledge Handbook of Security Studies*, Myriam Dunn Cavelty and Victor Mauer (editors), New York, Routledge, 2009, pp.180-189, nas pp.182-183.

ganhar as guerras sem necessidade de as travar, as chamadas «guerras limpas». De facto, os militares russos foram os primeiros a identificar o problema da Revolução nos Assuntos Militares (RMA) em curso nos Estados Unidos, percebendo que este processo obrigaria a ex-União Soviética a uma rápida e radical modernização para contrariar o superior domínio da informação e da sua transformação em conhecimento alcançados por Washington. Nessa altura a possibilidade de vir a ocorrer uma ciberguerra, então definida como um ciberataque de natureza militar contra um Estado inimigo, era encarada como um desenvolvimento estratégico que, a consumir-se, poderia contrariar a proteção dos interesses estratégicos nacionais da URSS, já que era evidente que o país não estava a conseguir acompanhar o ritmo dos desenvolvimentos tecnológicos americanos neste domínio⁸.

O teor da Resolução apresentada pela Rússia não surpreendeu os países membros da Comissão. Não era esta a primeira vez que Moscovo recorria a este tipo de expediente político em matérias relacionadas com o controlo de armamentos e desarmamento com o objetivo de travar a superioridade norte-americana num ou outro tipo de tecnologia militar em que os Estados Unidos pudessem ter a dianteira tecnológica. Na carta que acompanhava a proposta de Resolução é dito que a resolução pretendia evitar conflitos no ciberespaço e uma corrida às ciberarmas, o mesmo é dizer, o principal objetivo político da Resolução era contrariar um uso do ciberespaço contrário ao objetivo de manter a paz e a segurança internacionais. A Resolução propunha um inventário das tecnologias de informação a fim de evitar o seu uso militar, sugerindo-se que o seu emprego poderia equivaler ao uso de armas de destruição em massa (WMD). Mas para acomodar as preocupações políticas de outros países, nomeadamente dos países ocidentais, foi acrescentado ao texto uma referência adicional à proibição do uso do ciberespaço «por criminosos e terroristas». Deste modo, a Resolução consegue enquadrar no seu mandato todo o espectro das ciberameaças – a ciberagressão, o ciberterrorismo patrocinado ou não pelos Estados, os fenómenos de cibercriminalidade, a questão das ameaças às infraestruturas críticas e ainda o problema da intervenção nos assuntos

⁸ ENEKEN TIKK e MIKA KERTTUNEN, *The Alleged Demise of the UN GGE: An Autopsy and Eulogy*, New York, Cyber Policy Institute, 2017, p. 8.

internos dos Estados. Dada a sua abrangência, a resolução pôde ser facilmente adotada por consenso⁹.

Assim, numa primeira fase, entre os anos de 1999 e 2003, Washington permaneceu naturalmente focado no uso criminoso e terrorista do ciberespaço, dado que os ataques do dia 11 de setembro de 2001 ao território americano dominavam as suas preocupações de política externa. Entretanto, anos mais tarde Washington acabaria por rever esta prioridade inicial por força de mudanças no ambiente estratégico que impactaram na definição do interesse nacional americano. As razões para esta mudança de orientação serão explicadas mais adiante neste texto.

A aprovação da Resolução A/RES/53/70 deu origem à constituição de seis Grupos de Peritos Governamentais das NU sobre NU sobre Desenvolvimentos no Campo Da Informação e Telecomunicações no Contexto da Segurança Internacional (*Groups of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*. UN GGEs), tendo o Primeiro GGE iniciado os seus trabalhos em 2004.

Estes Grupos de Peritos, cinco deles liderados pela Rússia e que contaram sempre com a participação dos cinco Membros Permanentes do Conselho de Segurança (P5) e de outros países relevantes, como a Alemanha, experimentaram avanços e retrocessos, mas sobretudo contribuíram significativamente para dar visibilidade à existência de divergências profundas na comunidade internacional acerca dos desafios colocados pelo ciberespaço no plano político-militar.

O objetivo da criação do Primeiro Grupo de Peritos era discutir o controlo das armas informacionais, dado que na perspetiva russa o ciberespaço configurava um problema de segurança da informação. Mas quando o Primeiro Grupo de Peritos começou efetivamente a trabalhar a realidade estratégica do mundo tinha mudado radicalmente. Efetivamente no ano de arranque do GGE, em 2004, os grandes Estados já tinham uma presença estratégica no ciberespaço¹⁰, passando a ser prioritário a definição das normas

⁹ ENEKEN TIKK-RINGAS, *Developments in the Field of Information and Telecommunication in the Context of International Security: Work of the UN First Committee 1998-2012*, Grand Saconnex, ICT4Peace Publishing, 2012, p.4.

¹⁰ TIKK e KERTTUNEN, *The Alleged Demise*, cit. p.9.

que permitissem regular o seu comportamento em ambiente ciber. Por esta razão fundamental deixou de fazer sentido prosseguir com o objetivo inicial de proibir a utilização deste teatro de operações pelos grandes poderes.

Os GGE receberam mandato para, entre outros aspetos, clarificar a adaptabilidade dos princípios de DIH ao espaço digital, nomeadamente o princípio da humanidade, que proíbe causar todo o tipo de sofrimento, lesão ou destruição desnecessários para conseguir o propósito legítimo de um conflito; o princípio da necessidade militar; o princípio da proporcionalidade; o princípio da distinção entre combatentes e não combatentes e o princípio da precaução¹¹.

Os GGE reuniam em Genebra ou em Nova Iorque, com uma composição variável, congregando entre quinze e vinte e cinco Estados¹². A aprovação dos seus Relatórios (Conclusões e Recomendações) era feita por consenso.

3. Os Grupo de Peritos Governamentais

3.1. Primeiro Grupo de Peritos Governamentais (2004/2005)

Constituído por quinze membros, foi liderado pela Rússia e contou com a participação dos Estados Unidos, França e Reino, entre outros países. Este GGE discutiu o impacto do desenvolvimento das tecnologias de informação e comunicação na segurança nacional¹³. Como referido, as transformações operadas no sistema internacional desde a aprovação da Resolução acabaram por determinar uma mudança de estratégia dos proponentes da Resolução. Nesta altura era bem evidente que a Rússia, China, Estados

¹¹ ADINA PONTA, «Responsible Behavior in Cyberspace: Two New Reports form Parallel UN Processes», *ASIL Insights*, vol.25: 14, July 30, 2021, p.3, disponível em <https://www.asil.org/insights/volume/25/issue/14> (consulta feita em 24 de novembro de 2022).

¹² WILPE, *Cyber Peace and Security*, disponível em <https://reachingcriticalwill.org/resources/factsheets/critical-issues/14010-cyber-peace-and-security> (consulta feita em 4 de janeiro de 2023).

¹³ LUCAS TANGLEN e REYMOND YAMMINE, *The Colapse of UN Talks on the Application of International Law in Cyberspace: Why It Matters to US Business*, K& L Gates, 24 May 2018, disponível em <https://www.klgates.com/The-Collapse-of-UN-Talks-on-the-Application-of-International-Law-in-Cyberspace-Why-It-Matters-to-US-Businesses-05-24-2018> (consulta feita em 24 de novembro de 2022).

Unidos e Israel já tinham presença no ciberespaço. Consequentemente a ideia de proibir a utilização do ciberespaço por parte dos Estados mais avançados do ponto de vista tecnológico deixara de fazer sentido. Por isso, o Primeiro GGE acabaria por centrar o seu trabalho na discussão dos aspetos concretos relacionados com a regulação da sua utilização. O GGE discutiu o direito de os Estados assegurarem a segurança da informação sem limitações e a adoção de um novo regime internacional sobre a matéria, prioridades defendidas em primeira linha pela Rússia, China e Bielorrússia. Esta posição foi desde o primeiro minuto fortemente contestada pelos Estados Unidos e União Europeia (EU). Este ambiente altamente divisivo inviabilizou a obtenção de um acordo sobre o texto do Relatório final do Primeiro GGE, que nunca chegou a ser aprovado¹⁴.

3.2. Segundo Grupo de Peritos Governamentais (2009/2010)

Os trabalhos do Segundo GGE iniciaram-se em 2009, num momento em que a Estónia e a Geórgia já tinham sofrido ciberataques politicamente motivados com origem na Rússia. Estes desenvolvimentos foram determinantes para o Ocidente começar a valorizar de outra forma a questão das ameaças à segurança da informação, tal como ficou plasmado no Relatório Final deste Grupo adotado por consenso em 2010 (A/65/201, de 30 julho)¹⁵. É significativo que tenha sido por esta altura (2009) que os Estados Unidos decidiram aprovar a sua primeira política para o ciberespaço.

Um ano depois da aprovação do Relatório, em setembro de 2011, numa proposta conjunta de quatro países pertencentes à Organização de Cooperação de Xangai (China, Rússia, Tajiquistão e Uzbequistão) a Rússia lançou a ideia de um Código Internacional sobre Segurança da Informação (A/66/359, de 14 de setembro, revista em 2015). Este modelo de regulação, embora seja mais flexível que um tratado por ser um instrumento de *soft law*, não logrou o apoio de muitos países. Os Estados Unidos, em particular, manifestaram desde logo o seu frontal desacordo em relação à ideia de negociar um Código desta natureza.

¹⁴ TIKK e KERTTUNEN, *The Alleged Demise*, cit., p. 8.

¹⁵ TIKK e KERTTUNEN, *The Alleged Demise*, cit. p.10.

3.3. Terceiro Grupo de Peritos Governamentais (2012-2013)

O Relatório Final aprovado por consenso em 2013 (A/68/98 de 24 de junho) mantém a tensão que desde o início está presente no trabalho da Primeira Comissão e que se traduz na aparente impossibilidade de compatibilizar a perspectiva liberal dos Estados Unidos sobre o uso do ciberespaço e o posicionamento soberanista da Rússia e China. Esta oposição fundamental que tem marcado o quadro geral de relacionamento estratégico entre estas potências é, no caso vertente, sem dúvida agravado pelas características muito próprias da realidade virtual, que se assume como um espaço único, de natureza não territorial.

O Relatório afirma, como princípio geral, que a aplicação das normas do DI no ciberespaço, nomeadamente a Carta das NU, é uma medida fundamental de redução de riscos que podem colocar em causa a paz, segurança e a estabilidade internacionais. Não obstante esta posição de princípio, o Relatório é muito claro quanto à necessidade de uma clarificação – que deveria acontecer em momento posterior – acerca do modo como essas normas se aplicam aos comportamentos dos Estados e que, devido às peculiaridades do ciberespaço, poderá vir a haver necessidade de criar normas adicionais. Outro ponto controvertido do Relatório é a questão do exercício da soberania no ambiente virtual. Neste ponto, o relatório reafirma o princípio da soberania dos Estados na condução de atividades de proteção de infra-estruturas que se situem nos territórios desses Estados¹⁶.

3.4. Quarto Grupo de Peritos Governamentais (2014/2015)

O Quarto Grupo de Peritos dedicou-se ao estudo de como as normas, regras e princípios de comportamento responsável dos Estados acordados em 2013 poderiam ser operacionalizados. O Relatório Final aprovado por consenso (A/70/174, de 22 de julho de 2015) estabelece onze recomendações de normas voluntárias não vinculativas, regras e princípios de comportamento responsável. Também se chegou a acordo sobre a necessidade de Medidas

¹⁶ TIKK e KERTTUNEN, *The Alleged Demise*, cit., p.11; UNITED NATIONS, *United Nations, Cyberspace*, cit., p.18.

para a Criação de Confiança (CBM), o reforço da cooperação internacional e reconheceu-se a importância de apoiar a capacitação dos Estados nestas questões¹⁷.

Os Estados deveriam observar vários princípios de DI inscritos na Carta das NU como respeitar a soberania dos outros Estados, promover a resolução de disputas por meios pacíficos e não violar o princípio de não intervenção nos assuntos internos dos outros Estados¹⁸. A Assembleia Geral pediu aos Estados que seguissem estas recomendações, mas a formação de um consenso para orientar o conteúdo das normas que seriam aplicadas no quadro da regulação internacional do ciberespaço tem-se revelado problemática, pela circunstância de os países continuarem a manter entendimentos muito díspares sobre o seu conteúdo.

3.5. Quinto Grupo de Peritos Governamentais (2016/2017)

Em 2017, não houve consenso para aprovar o Relatório Final deste GGE¹⁹. Isto aconteceu porque a fórmula de compromisso ensaiada pelos grupos anteriormente constituídos era demasiado frágil para poder sobreviver a dúvidas que se adensavam sobre o melhor formato de discussão destas questões a adotar no futuro, o que levou à discussão de possíveis fóruns e entidades alternativas de negociação e também à conclusão de que seria preciso envolver mais *stakeholders* no quadro de uma maior transparência nos trabalhos²⁰.

Também em termos substantivos começou a ser notório que a crescente divergência de perspetivas defendidas pelos principais ciberpoderes em

¹⁷ DAN EFRONY, *The UN Cyber Groups, GGE and OEWG: A Consensus is Optimal, But Time is of the Essence*, Justsecurity.org, July 16, 2021, disponível em <https://www.justsecurity.org/77480/the-un-cyber-groups-gge-and-oewg-a-consensus-is-optimal-but-time-is-of-the-essence/> (consulta feita em 3 de novembro de 2023).

¹⁸ UNITED NATIONS, *Developments in the Field of Information and Telecommunications in the Context of International Security*, New York, United Nations Office for Disarmament Affairs (UNODA) Fact Sheet, 2019, p. 2, disponível em <https://www.dfat.gov.au/sites/default/files/unoda-information-security-fact-sheet.pdf> (consulta feita em 3 de novembro de 2023).

¹⁹ EFRONY, *The UN Cyber Groups*, cit..

²⁰ TIKK e KERTTUNEN, *The Alleged Demise*, cit., p.15 e ss.

relação às questões de Direito Internacional acabaria por impedir a possibilidade de alcançar consensos satisfatórios. Um dos maiores desafios para os Estados que participaram neste GGE foi, portanto, a extrema dificuldade de consolidar a ideia da aplicabilidade do Direito Internacional ao ciberespaço. Considerando as barreiras e dificuldades políticas da regulação em ambiente virtual, nesta altura os pontos mais controvertidos eram: em primeiro lugar, a questão da aplicação do DIH; em segundo lugar, o problema das contramedidas, também muito discutidas e ainda, não menos importante, a polémica questão do direito à legítima defesa em ambiente digital²¹.

Sobre este último assunto, a posição que o governo norte-americano tem sustentado é a de que o reconhecimento da aplicação do Artigo 2.º, nº 4 da Carta das NU implica necessariamente – como consequência lógica da proibição de ameaça ou uso da força – a possibilidade de exercício do direito à legítima defesa (Artigo 51.º da Carta), desde que cumpridos determinados requisitos. Porquanto permite clarificar de que modo os Estados podem ou não responder a ciber-incidentes, esta solução tem a vantagem de criar expectativas estáveis na relação entre os Estados o que, na ótica norte-americana, ajudaria a reduzir o risco de incidentes. Com uma perceção diametralmente oposta, países como a China, Rússia e Cuba defendem que a aplicação do Artigo 51.º no ambiente ciber pode transformar o ciberespaço num teatro de operações militares onde podem ser impostas sanções, nomeadamente as medidas mais gravosas de todas, a possibilidade de sanções de natureza militar. Para estes países tal solução é a todos os títulos inadmissível na medida em que conduz irremediavelmente a uma situação de militarização do ciberespaço²².

3.6. Sexto Grupo de Peritos Governamentais (2019-2021)

Até 2019, os GGE constituíam-se como os únicos fóruns onusianos de discussão das dimensões jurídicas, políticas e tecnológicas do ciberespaço no contexto da segurança internacional.

²¹ TIKK e KERTTUNEN, *The Alleged Demise*, cit., p.15 e ss..

²² TANGLEN e YAMMINE, *The Collapse of UN Talks*, cit.; KERSTIN VIGNARD e CAMINO KAVANAGH, *The UN GGEs on ICTS and International Security*, New York, United Nations/UNIDIR, s.d. p. 4; TIKK e KERTTUNEN, *The Alleged Demise*, cit., p.15 e ss..

No entanto, era evidente que estava em curso uma profunda mudança no mundo e que este já não encontrava no modelo dos GGE uma resposta satisfatória à necessidade de pensar a regulação do ciberespaço no domínio da segurança. Como se viu, o Quinto GGE não logrou a aprovação de um Relatório Final: em 2017 vivia-se um tempo de tensões e incertezas relacionadas com várias ciberoperações hostis contra membros do GGE, algumas com alegada origem na Rússia²³, o que inviabilizou a obtenção de um consenso sobre o texto a aprovar. Por esta razão, a Rússia deu-se conta que o modelo dos GGE estava esgotado e que era preciso criar um modelo de discussão mais inclusivo, que garantisse maior transparência. É assim que em 2018 a Rússia propõe a criação de um Grupo de Trabalho Aberto das NU sobre Desenvolvimentos no Campo da Informação e Telecomunicações no Contexto da Segurança Internacional (*UN Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security*, UN OEWG, A/RES/73/27, de 11 de dezembro, mais tarde redenominado *UN OEWG on Security of And in The Use of Information and Communications Technologies*), aberto a todos os Estados membros que nele quisessem participar. A AGNU aprovou a sua criação por cento e vinte e quatro votos a favor, seis votos contra e quarenta e oito abstenções. Em relação à temática não se registam mudanças, a Rússia mantém-se focada no uso militar do ciberespaço e preocupada com o impacto do desenvolvimento das TIC na segurança nacional e internacional e nos assuntos militares²⁴.

É neste contexto que os Estados Unidos decidem patrocinar o que viria a ser o Sexto Grupo de Peritos (agora *Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security*), aprovado pela Resolução 73/266 de 28 de dezembro de 2018, que obteve cento e sessenta e um votos a favor, dez votos contra e oito abstenções. Assim, a aprovação de duas Resoluções concorrentes foi apenas possível porque houve um conjunto expressivo de setenta e sete países que votaram favoravelmente as duas Resoluções, apesar de estas Resoluções proporem modelos de regulação substancialmente diferentes. Embora seja

²³ PONTA, «Responsible Behavior...», cit., p. 4.

²⁴ EFRONY, *The UN Cyber Groups*, cit..

importante realçar que a Resolução americana recebeu mais votos positivos do que a Resolução introduzida pela Rússia²⁵. Em qualquer caso, parece-nos que o fato de existir uma diferença de votos na votação das duas Resoluções não nos permite antecipar de forma segura qual será o paradigma de regulação do ciberespaço que a Assembleia Geral acabará por adotar no futuro.

Importante é não esquecer que foi impossível fundir os dois processos, apesar de os mandatos do GGE e do OEWG serem globalmente muito semelhantes. Isto significa que os países de inclinação liberal defendem uma visão da cooperação internacional no ciberespaço aparentemente inconciliável com a visão dos russos e chineses. Nestes anos críticos, o confronto de visões no Sexto GGE foi igualmente muito evidente, ao ponto de temporalmente o Relatório produzido pelo Grupo de Peritos ter sido publicado pouco tempo depois do Relatório do novo OEWG ter sido apresentado.

Por outro lado, agora que a liderança do Sexto GGE é assumida pelos norte-americanos é natural que o Relatório (A/76/135, de 14 de julho), aprovado em 2021 por consenso e estruturado em sete secções semelhantes ao Relatório do OEWG, vá mais longe no seu alcance do que o texto produzido por este último. No seio deste GGE, os países que partilham valores democráticos trabalharam juntos no sentido de impor consequências àqueles que violam as normas de comportamento responsável no ciberespaço, procurando consolidar e cumprir normas em vigor. Vejamos agora em pormenor alguns dos aspetos mais importantes a que o Relatório faz referência.

Primeiramente, vemos que a responsabilização dos Estados por atividades cibernéticas maliciosas aplica-se a operações ciber no conflito armado, ao nível do DIH, invocando-se os princípios da humanidade, necessidade, proporcionalidade e distinção²⁶. Note-se, porém, que o Relatório reconhece que é preciso mais diálogo para qualificar termos-chave nesta dimensão virtual da realidade, o que significa que continua a haver desacordo sobre a sua aplicação concreta no ambiente virtual. Também se nota uma hesitação em determinar a natureza de obrigações de *due diligence* que derivam do princípio da soberania dos Estados – no sentido de assegurar que o território ou as infraestruturas críticas sob controlo do Estado não são usadas para

²⁵ EFRONY, *The UN Cyber Groups*, cit..

²⁶ PONTA, «Responsible Behavior in Cyberspace», cit., p. 4.

operações que afetem os direitos – e produzam graves consequências adversas – de outros Estados²⁷. Enquanto nos Relatórios de 2013 e 2015 esta questão era voluntária, agora parece existir uma expectativa ampla e de senso comum de que os Estados tentarão fazê-lo e que devem dar assistência aos Estados que não tenham essa capacidade, o que pode ajudar a abrir caminho a que venha a ser reconhecida como uma regra de Direito Internacional, no futuro.

Por outro lado, e ao contrário do OEWG, o Relatório de 2021 expande os princípios de DI que podem vir a ser relevantes no ciberespaço. Recorde-se que o Relatório de 2015 reafirmava a noção de igualdade soberana dos Estados como a principal norma a observar. Já o texto do Relatório de 2021 afirma que há proibição de ameaça ou uso da força contra a integridade territorial ou independência política dos Estados, que existe uma obrigação de respeitar os DH e liberdades fundamentais e que é preciso respeitar o princípio de não intervenção nos assuntos internos²⁸.

Outro aspeto desde sempre controvertido a que o Relatório alude tem que ver com a vulnerabilidade das infraestruturas críticas. Neste ponto, o Relatório sublinha a ideia de que não há proteção sem regulação, favorecendo a ligação desta necessidade de proteção à questão do capacitação e ainda à necessidade de aprofundar a cooperação entre os Estados e entre o sector público e o sector privado. Na visão do Relatório, o cumprimento das normas enunciadas em 2015 exige, portanto, que se aprofundem três eixos fundamentais: a cooperação internacional, as CBM e a capacitação. Existe, contudo, um grupo de países que têm reservas em relação a alguns destes aspetos, nomeadamente no que tange o trabalho da OSCE em termos de CBM havendo ainda dúvidas sobre como se pode financiar esta capacitação²⁹.

A realidade política nestes anos é, em resumo, muito complexa, porquanto neste período o GGE e o OEWG trabalharam de forma paralela e muitos países eram muito ativos em ambos os grupos, apesar das diferenças de perspetiva sobre o modelo de governação. Quando finalmente, em 2021, o Grupo de Peritos deu por encerrado os seus trabalhos, houve uma clarificação desta situação, tendo sido possível ao OEWG passar a assumir a partir desse

²⁷ PONTA, «Responsible Behavior in Cyberspace», pp. 4-5.

²⁸ PONTA, «Responsible Behavior in Cyberspace», cit, p. 5.

²⁹ PONTA, «Responsible Behavior in Cyberspace», cit., p.5.

mesmo momento a responsabilidade de promover o aprofundamento do tema do uso responsável do ciberespaço pelos Estados³⁰.

4. Os OEWG

4.1. Primeiro Grupo de Trabalho Aberto (2018-2021)

A criação do primeiro OEWG é um passo importante para a regulamentação do ciberespaço em razão de ter sido o primeiro órgão das NU a debater assuntos de cibersegurança com a possibilidade de participação de todos os Estados membros. Também permitiu de algum modo a inclusão a sociedade civil e não tomava decisões de forma fechada.

O Relatório final que produziu em 2021 (A/76/135, de 14 de julho) foi aprovado por consenso o que constitui um bom sinal político depois de em 2018 nos termos deparado com dois processos negociais sobre esta mesma questão que corriam em paralelo.

Participaram nos trabalhos deste Grupo sessenta e oito países³¹. O Relatório confirmou o *acquis* (o que foi afirmado nos Relatórios adotados por consenso dos três GGE, em 2010, 2013 e 2015, respetivamente), embora seja motivo de discussão os seus exatos termos³². De facto, neste relatório reafirma-se inequivocamente que o DI se aplica ao ciberespaço, incluindo as disposições da Carta das NU, mas é omissivo sobre que leis se aplicam e de que modo podem ser aplicadas. O Relatório apenas refere que os Estados devem partilhar perspetivas e práticas, devendo indicar que assuntos específicos de DI necessitam ser aprofundados. A frontal oposição da China³³, Cuba e Bielorrússia à inclusão do DIH, por exemplo, mostra como continua a ser muito controversa a aplicação dos princípios da humanidade, necessidade, proporcionalidade, distinção e precaução ao nível do DIH no ciberespaço³⁴.

³⁰ GENEVA DIG WATCH, *First Report of the UN OEWG on Cybersecurity*, Geneva Internet Platform, Diploforum, 2023, disponível em <https://dig.watch/?s=+the+first+OEWG++/> (consulta feita em 1 de novembro de 2023).

³¹ PONTA, «Responsible Behavior in Cyberspace», cit., p. 2.

³² GENEVA DIGITAL WATCH, *First Report*, cit..

³³ XINCHUCHU GAO, «An Attractive Alternative? China's Approach to Cyber Governance and Its Implications for the Western Model», *The International Spectator*, vol. 57, nº 3, 2022, pp.15-30, na p.23.

Devido a estas tensões, alguns aspetos não surgem especificamente referidos no Relatório, como por exemplo o cibercrime, a questão da governação internacional, a legítima defesa, o DIH e os DH³⁵. Ora, estas exclusões contrastam com o teor dos relatórios anteriores dos GGE e contrariam os discursos proferidos durante os trabalhos do OEWG: em ambos os casos estas questões encontravam-se bastante mais clarificadas. Outro aspeto a referir sobre este Relatório é a forte valorização da dimensão soberana dos Estados em matéria de capacitação, se o compararmos com o texto do Relatório do Sexto GGE.

Para além do Relatório Final substantivo, o outro produto do Grupo de Trabalho é o Sumário do Presidente, que elenca os assuntos sobre os quais não se conseguiu chegar a consenso – nomeadamente tópicos como o problema da atribuição, a aplicação do DIH e uma clara integração dos processos eleitorais na questão das infraestruturas críticas, entre outros³⁶. Este último ponto introduz a questão da propaganda hostil e das campanhas difamatórias com o objetivo de interferir nos assuntos internos dos Estados, nomeadamente nos processos eleitorais, comportamento que a Rússia tem sido acusada de instigar em muitos países.

Este complexo *puzzle* político é, acima de tudo, um reflexo da tensão que opõe os países que contestam a aplicação do DIH e que são geralmente defensores de um instrumento jurídico vinculativo – grupo liderado pela Rússia – e um conjunto de países no qual se destacam os Estados Unidos, Austrália e a própria UE, para quem é suficiente regular a partir do *acquis* e das normas existentes³⁷.

4.2. Segundo OEWG (2021-2025)

Com mandato renovado para o período 2021-2025 (A/RES/75/240 de 4 de janeiro de 2021), espera-se que o segundo Relatório do OEWG seja entregue em 2025.

³⁴ PONTA, «Responsible Behavior in Cyberspace», cit., p. 3.

³⁵ ALLISON PYTLAK, «A Win for Diplomacy: Questions Remain for Cyber Peace», *Cyber Peace & Security Monitor*, vol. 1, nº 10, 17 March 2021, disponível em <https://www.reachingcriticalwill.org/images/documents/Disarmamentfora/other/icts/monitor/CyberMonitor1.10.pdf> (consulta feita em 28 de outubro de 2023).

³⁶ PONTA, «Responsible Behavior in Cyberspace», cit. p. 4.

³⁷ PYTLAK, «A Win for Diplomacy...», cit..

5. Manobras Diplomáticas Recentes

A necessidade de garantir a continuidade dos trabalhos após a entrega do Relatório do Segundo OEWG motivou a aprovação pela Primeira Comissão de um Programa de Ação (PoA)³⁸ (A/C.1/77/L.73), em 12 de outubro de 2022. Concebido para funcionar de forma permanente, constitui-se como um mecanismo inclusivo orientado para a ação após o encerramento das atividades do Segundo OEWG, previsto como se disse acima para o ano de 2025³⁹.

O PoA foi copatrocinado por quarenta países a partir de uma iniciativa da França e Etiópia. Será o primeiro fórum permanente dedicado à discussão do papel das TIC no contexto da segurança internacional, propondo-se analisar as ameaças existentes e potenciais; estudar medidas de apoio à capacitação e medidas que permitam implementar os compromissos de uso responsável pelos Estados, bem como promover o empenhamento e a cooperação entre as partes interessadas mais relevantes. Também tem mandato para proceder à revisão periódica da implementação do PoA. Votaram a favor deste Plano cento e cinquenta e sete países. China, Rússia, Irão, Síria, Coreia do Norte, Nicarágua votaram contra e houve catorze abstenções⁴⁰

Esta iniciativa deu recentemente origem a uma contraproposta russa que consiste na proposta de negociação de uma convenção sobre segurança da informação⁴¹ destinada a reafirmar que o ciberespaço não está desconectado

³⁸ UNITED NATIONS, *Working Paper for a Programme of Action (PoA) to Advance Responsible State Behavior in the Use of ICTs in the Context of International Security*, março de 2023, disponível em <https://documents.unoda.org/wpcontent/uploads/2021/11/Working-paper-on-the-proposal-for-a-Cyber-PoA.pdf> (consulta feita em 23 de outubro de 2023).

³⁹ REACHING CRITICAL WILL, *Information and Communications Technology (ICT)*, disponível em <https://www.reachingcriticalwill.org/disarmament-fora/ict> (consulta feita em 20 de novembro de 2023).

⁴⁰ PAUL MEYER, *Cyber Security at the UN General Assembly First Committee: Déjà vu all over again*, ICT for Peace, 11 de novembro de 2022, disponível em <https://ict4peace.org/activities/cyber-security-at-the-un-general-assembly-first-committee-deja-vu-all-over-again/> (consulta feita em 20 de janeiro de 2023).

⁴¹ RUSSIAN FEDERATION, *Updated Concept of the Convention of the United Nations on Ensuring International Information Security*, disponível em [https://docslibrary.unoda.org/OpenEnded_Working_Group_on_Information_and_Communication_Technologies_\(2021\)/ENG_Concept_of_UN_Convention_on_International_Information_Security_Proposal_of_the_Russian_Federation.pdf](https://docslibrary.unoda.org/OpenEnded_Working_Group_on_Information_and_Communication_Technologies_(2021)/ENG_Concept_of_UN_Convention_on_International_Information_Security_Proposal_of_the_Russian_Federation.pdf) (consulta feita em 3 de novembro de 2023).

da soberania estatal. Esta manobra diplomática procura esvaziar a possibilidade de dar centralidade política ao PoA, como é vontade da generalidade dos países ocidentais, pretendendo garantir que depois da extinção do OEWG a Rússia assuma a condução das negociações da convenção por ela proposta.

Para proteger as suas ciber-fronteiras, a Rússia quer reafirmar o princípio da igualdade soberana, a integridade territorial e a não ingerência nos assuntos internos dos outros países através de propaganda e outros meios semelhantes⁴² – isto apesar de a Rússia recorrer extensivamente a este expediente. Como se viu anteriormente, a Rússia não reconhece a aplicação do DIH ao ciberespaço. Sob pretexto da necessidade de os Estados atuarem mais fortemente no controlo do ciberespaço é reforçada a visão de que o que verdadeiramente interessa é manter a estabilidade económica e social – uma necessidade premente para qualquer Estado autoritário. Com consciência de que o ciberespaço é entendido pelos países democráticos como um espaço de liberdade, o texto omite o direito à privacidade como um dos mais importantes DH e não enfatiza o direito à liberdade de expressão e de reunião. Aliás, a referência aos DH apenas surge no texto a propósito da liberdade de expressão e apenas para ser restringida por questões de segurança nacional, ordem pública e razões morais⁴³.

Em suma, a Rússia e a China desejam uma nova regulamentação e um criterioso controlo nacional da informação que entra, sai e circula e que pode pôr em causa a segurança nacional e os fundamentos políticos, económicos e sociais das nações⁴⁴.

6. Conclusões

A aprovação da Resolução «Desenvolvimentos no Campo da Informação e Telecomunicações no Contexto da Segurança Internacional» permitiu à Primeira Comissão da AGNU empenhar-se na discussão dos aspetos

⁴² VALENTIN WEBER, *The Dangers of a New Russian Proposal for a UN Convention on International Information Security*, The Council of Foreign Relations, March 21, 2023, disponível em <https://www.cfr.org/blog/dangers-new-russian-proposal-un-convention-international-information-security> (consulta feita em 1 de dezembro de 2023).

⁴³ WEBER, *The Dangers of a New Russian Proposal*, cit..

⁴⁴ TIKK e KERTTUNEN, *The Alleged Demise*, cit., pp.32-33.

político-estratégicos do desenvolvimento de um ciberespaço previsível, estável e seguro.

Com este objetivo, os seis Grupos de Peritos Governamentais e os dois Grupos de Trabalho criados pela Primeira Comissão têm discutido vários problemas do ciberespaço, sendo um dos temas mais importantes a possibilidade de guerras no ciberespaço ou a partir do ciberespaço e a questão da aplicação do DIH no ambiente ciber.

Como se tentou demonstrar neste artigo, atualmente a regulação do ciberespaço é um novo campo de batalha ideológica que opõe um grupo de países liberais liderados pelos Estados Unidos à Rússia e China. No debate sobre a questão de um conflito ocorrer no ciberespaço, os Estados Unidos e outros Estados com perspectivas liberais têm sustentando que as normas existentes de Direito Internacional, nomeadamente no quadro do DIH, se aplicam ao ambiente cinético. Nesse sentido, os Estados Unidos opuseram-se desde o início à ideia de negociar uma convenção sobre segurança no ciberespaço, contrariando a posição que tem sido insistentemente defendida pela Rússia e acompanhada por outros países autocráticos que entendem que é necessário elaborar um novo instrumento juridicamente vinculativo sobre a questão. Também defendem, numa perspectiva mais ampla do ciberespaço, o fluxo livre da informação e do acesso a ela, a liberdade de expressão e a segurança das infraestruturas e redes. A Rússia, a China e outros países autocráticos, por seu lado, entendem que não existe o direito à legítima defesa (Artigo 51.º) em ambiente digital e priorizam o reforço da soberania digital dos Estados, através da implementação de leis que criam um ambiente mais controlado no ambiente internacional e permitem um criterioso controlo nacional da informação que entra, sai e circula que pode pôr em causa a segurança nacional e os fundamentos políticos, económicos e sociais dos países.

Entendemos como muito relevante a circunstância de os países que integram a Primeira Comissão da Assembleia Geral hesitarem no seu apoio a uma ou outra solução para regular estas atividades no ciberespaço. Assim, é de notar que uma confortável maioria viabilizou a criação dos cinco Grupos de Trabalho propostos pela Rússia onde a Rússia defendeu as suas posições soberanistas. Por outro lado, essa decisão não constituiu obstáculo a que se obtivesse uma votação expressiva a favor da formação do Sexto Grupo de Peritos agora liderado pelos Estados Unidos, da mesma maneira que os

países que integram a Comissão viabilizaram o PoA, uma iniciativa dos países liberais alinhados com os Estados Unidos. Importará neste quadro perceber como irá a Primeira Comissão reagir à recente proposta de negociação de uma convenção sobre segurança da informação apresentada em março de 2023 pela Rússia. Dadas as tensões acumuladas ao longo do tempo, este novo desenvolvimento vem apenas agudizar as evidentes dificuldades que este conturbado processo tem encontrado.

Observa-se uma militarização crescente do ciberespaço, não se podendo ignorar por mais tempo a possibilidade de um ciberconflito pode tornar-se realidade a partir da possibilidade de ocorrência de ataques cibernéticos (ainda que eventualmente acompanhados de um conflito em ambiente cinético, coordenado ou sucessivo). Acresce que os fenómenos relacionados com propaganda hostil, campanhas de desinformação e notícias falsas na *internet*, fenómenos que tendem a piorar em tempo de crise e guerra, colocam desafios importantes aos países que integram a Primeira Comissão.

Argumenta-se que diversas dinâmicas disputam presentemente o espaço político no interior da Primeira Comissão e que as hesitações dos seus membros podem ter um significado profundo que ultrapassa o mandato desta Comissão em relação ao aspetos político-estratégicos do ciberespaço.

Deste ponto de vista, não pode ignorar-se a crescente insatisfação de alguns países com o facto de um conjunto de países ocidentais terem desenhado e tradicionalmente dominado os mecanismos de governação da internet. Mais ainda, é inevitável que cada vez mais países ocidentais sejam forçados a pensar sobre o que significa a soberania na internet. Em suma, só perceberemos o que está realmente em causa nestas discussões se reconhecermos que as dinâmicas políticas na Primeira Comissão carecem de uma leitura mais ampla e profunda que extravasa a própria Comissão e que esta leitura em torno do da nova arquitetura política do ciberespaço deve ser necessariamente alicerçada num período de análise mais longo.

La debida diligencia y el derecho de legítima defensa frente al terrorismo: especial referencia al caso de la Franja de Gaza

Due diligence and the right of self-defense against terrorism: special reference to the case of the Gaza Strip

Raquel Regueiro Dubra

Resumen: Los atentados terroristas perpetrados por Hamás contra Israel el 7 de octubre desencadenaron una respuesta masiva por tierra, mar y aire en la Franja de Gaza, justificada por parte del Estado israelí bajo el argumento del ejercicio de un derecho de legítima defensa. Esta aportación analiza la naturaleza de obligación de diligencia debida y su operatividad en el marco del derecho de legítima defensa consagrado en el artículo 51 de la Carta de las Naciones Unidas frente al terrorismo, haciendo referencia a la intervención militar israelí en el territorio palestino ocupado.

Palabras clave: debida diligencia, legítima defensa, Hamás, Israel, Gaza.

Abstract: The terrorist attacks perpetrated by Hamas against Israel on October 7th triggered a massive response across the land, sea and air on the Gaza Strip, under the argument of the exercise of a right of self-defense. This contribution analyses the nature of the obligation of due diligence within the framework of the right of self-defense enshrined in article 51 of the Charter of the United Nations against terrorism, making reference to the Israeli military intervention in the Palestinian occupied territory.

Keywords: due diligence; Gaza; Hamas; Israel; self-defense.

Sumario: 1. Introducción. 2. Israel frente al terrorismo. 3. El derecho de legítima defensa y la dificultad de la necesaria atribución del ataque armado. 3.1 El *ataque armado* como requisito para el derecho de legítima defensa. 3.2. El principio de diligencia debida 4. El caso de la Franja de Gaza: ¿Qué respuesta de fuerza para qué derecho de legítima defensa? 4.1 La Franja de Gaza como territorio palestino ocupado e Israel como potencia ocupante. 4.2 La inexistencia del derecho de legítima defensa de la potencia ocupante en un territorio ocupado. 4.3 La

inoperatividad de la obligación de diligencia debida para la determinación de un incumplimiento del principio de prohibición del uso de la fuerza. 4.4 La proporcionalidad como requisito confirmatorio de medidas armadas sin fines defensivos. 5. Reflexiones finales.

1. Introducción

El argumento del ejercicio del derecho de legítima defensa avanzado por Israel para justificar sus operaciones militares en la Franja de Gaza desde el 7 de octubre de 2023 en respuesta a la operación *Inundación de al-Aqsa* desarrollada previamente por Hamás se fundamenta en una visión extensiva del concepto de «ataque armado» establecido en el artículo 51 de la Carta de las Naciones Unidas y de las posibilidades de su atribución. Así, aceptar el argumento israelí obligaría a revisar las normas existentes relativas al uso de la fuerza al desarrollarse la intervención en la Franja de Gaza, territorio palestino ocupado por Israel.

Esta contribución tiene como objetivo la valoración de la licitud de la intervención israelí a la luz del derecho de legítima defensa. Para ello, tras un breve repaso a las operaciones israelíes contra el terrorismo que precedieron la actual operación *Espadas de Hierro*, el estudio se centra en el concepto de «ataque armado» y en la dificultad de su atribución a un Estado cuando es cometido por un actor no estatal. El análisis hace igualmente hincapié en la diligencia debida como obligación internacional y como posible nueva causa de atribución de responsabilidad internacional. En un segundo tiempo, se examina la condición de territorio ocupado de la Franja de Gaza a pesar de la desconexión israelí del año 2005, la validez del argumento del derecho de legítima defensa y la inoperatividad de la obligación de diligencia debida en el marco de la actuación de movimientos de liberación nacional para el cumplimiento del requisito de «ataque armado». Esta investigación finaliza con una mención a la ausencia de proporcionalidad de la acción militar israelí.

2. Israel frente al terrorismo

La operación *Inundación de al-Aqsa* de 7 de octubre de 2023, que consistió en un ataque coordinado del Movimiento de Resistencia Islámica (Hamás) contra objetivos en Israel, marcó el inicio de la intervención militar israelí en la Franja de Gaza, inicialmente mediante bombardeos masivos contra su población para abrir el paso a acciones sobre el terreno. La operación llevada a cabo el 7 de octubre por Hamás no tiene precedentes, tanto por su complejidad como por su letalidad y el hecho que se dirigió – a diferencia de ataques anteriores – de forma indiscriminada contra la población israelí, sin distinguir entre objetivos militares y objetivos civiles¹. A la vez, desnudó por completo los fallos en los sistemas de inteligencia y defensa israelíes que se vieron totalmente sorprendidos y superados, siendo incapaces de evitar o limitar los efectos del ataque.

En un primer momento, Israel no alegó estar haciendo uso de un derecho de legítima defensa. Así, la carta del representante israelí ante las Naciones Unidas a la Presidencia del Consejo de Seguridad y al Secretario General² no hace mención alguna al artículo 51 de la Carta de las Naciones Unidas y, aunque establece la autoría del ataque perpetrado en organizaciones terroristas lideradas por Hamás, no atribuye dichos ataques a ningún Estado en particular, haciendo únicamente referencia al rol de Irán como patrocinador de Hamás. Es más, Israel reconoce a Hamás como el único responsable de dicho ataque y anuncia que actuará en cualquier medida necesaria para proteger a sus ciudadanos y su soberanía. No obstante, en sus discursos

¹ Cfr. CAROLA GARCÍA-CALVO y ÁLVARO VICENTE, «La operación “Inundación de al-Aqsa” de Hamás y sus repercusiones en el yihadismo global», *ARI*, 101/2023, pp. 1-7.

² Identical letters dated 7 October 2023 from the Permanent Representative of Israel to the United Nations addressed to the Secretary-General and the President of the Security Council, Doc. S/2023/7642, de 9 de octubre de 2023. Sobre la obligación y el formato de la información al Consejo de Seguridad por parte del Estado que alega estar actuando en ejercicio de un derecho de legítima defensa, cfr. JAMES A. GREEN, «The Article 51 Reporting Requirement of Self-Defense Actions», *Virginia Journal of International Law*, vol. 55, nº 3, pp. 563-624. Sobre la comunicación de actividades durante el conflicto al Consejo de Seguridad, cfr. DAVID BOSCO, «Letters from the Front Lines: State Communications to the U.N. Security Council During Conflict», *Columbia Journal of Transnational Law*, vol. 54, 2016, pp. 341-381.

públicos posteriores y en el marco de las reuniones del Consejo de Seguridad de las Naciones Unidas, Israel declaró estar haciendo uso de un derecho de legítima defensa contra Hamás, una afirmación que fue apoyada por una escasa cuarentena de Estados, sobre todo occidentales³, y obtuvo un rechazo masivo por parte de los Estados árabes⁴. Así, en su primera intervención ante el Consejo de Seguridad, el representante israelí calificó la intervención militar en la Franja de Gaza de *operación de rescate* para salvar el futuro de Israel y a la población de Gaza de sus salvajes tiranos y añadió: “[t]he Council must support Israel’s right to defend itself. [...] Supporting Israel’s right to defend itself means supporting Israel’s goal to eradicating those cancerous jihadists”⁵.

La invocación por parte de Israel del derecho de legítima defensa consagrado en el artículo 51 de la Carta de las Naciones Unidas como justificación para sus intervenciones armadas no es nueva. Así, el 29 de octubre de 1956, la intervención militar en Egipto que marcó el inicio de la segunda guerra árabe israelí se basó en el argumento de la necesidad de defensa contra los ataques perpetrados por los fedayines egipcios, al considerar que Egipto apoyaba y alentaba dichas operaciones y era, por lo tanto, responsable de las mismas⁶. La presencia de *Hezbollah* en el Líbano y la de la *Yihad* islámica en Siria propiciaron ataques de Israel contra ambos Estados en repetidas ocasiones⁷.

En su relación con la resistencia palestina, el bombardeo por parte de Israel del aeropuerto de Beirut el 28 de diciembre de 1968 respondía – según Israel – al ataque llevado a cabo dos días antes por el Frente Popular para la Liberación de Palestina contra un avión comercial israelí en el aeropuerto de Atenas⁸; un ataque que el Líbano había permitido. En el mismo orden

³ Entre ellos, los miembros del Consejo de Seguridad: Estados Unidos, Reino Unido y Malta, véase S/PV/9439, de 16 de octubre de 2023.

⁴ Como expresó Jordania en el Consejo de Seguridad en nombre del grupo de Estados árabes, *Ibidem*.

⁵ *Ibid.*, p. 11.

⁶ Cfr. S/PV. 748, de 29 de octubre de 1956, p. 11, párr. 71.

⁷ Cfr. Carta de fecha 27 de enero de 2003 dirigida al Secretario General por el Representante Permanente de Israel ante las Naciones Unidas, A/57/717-S/2003/96; S/PV. 4836, de 5 de octubre de 2003, pp. 5-7; S/PV. 5489, de 14 de julio de 2006.

⁸ Cfr. S/PV. 1460, de 29 de diciembre de 1968, párrs. 27-28.

de ideas, Israel llevó a cabo una primera invasión del Líbano en marzo de 1978 como respuesta a un ataque por parte de la Organización para la Liberación de Palestina (OLP) contra un autobús en Israel y una segunda invasión el 6 de junio de 1982 tras la tentativa de asesinato del Jefe de Misión israelí en Londres el 3 de junio⁹. El 1 de octubre de 1985, las fuerzas de defensa israelíes (FDI) bombardearon tres edificios en *Borj-Cedria* (Túnez) al motivo que era el cuartel general de la OLP¹⁰.

No obstante, el argumento de la legítima defensa no fue bien recibido por parte de los demás Estados miembros de las Naciones Unidas. El Consejo de Seguridad condenó por unanimidad el bombardeo del aeropuerto de Beirut por parte de Israel en diciembre de 1968¹¹; pidió la retirada israelí del Líbano tras su invasión en 1982¹² y calificó de «acto de agresión armada» la operación en Túnez de 1985¹³. La dificultad de atribuir acciones de grupos armados no estatales a un Estado y la evidente falta de proporcionalidad en las respuestas armadas israelíes invalidaron la justificación del ejercicio de un derecho de legítima defensa en los términos establecidos por el artículo 51 de la Carta y el derecho consuetudinario.

El advenimiento de Hamás y su control de la Franja de Gaza desde su victoria en las elecciones legislativas del año 2006 reforzaron las capacidades militares del grupo (Brigadas *Izzadim Al Quassam*) que, solo o juntamente con otros grupos – como la *Yihad* Islámica y su brazo armado, las *Brigadas Al-Quds* – llevó a cabo sucesivos ataques contra objetivos israelíes. Por ello, la actual operación israelí «Espadas de hierro» sucede a las anteriores operaciones militares «Plomo Fundido» (2008), «Pilar Defensivo» (2012), «Margen Protector» (2014) o «Guardián de los Muros» (2021) que consistieron en el ataque masivo de objetivos en la Franja alegando un derecho de legítima defensa.

No obstante, la invocación del derecho de legítima defensa por parte de Israel suscita una serie de cuestiones que obligan a valorar su adecuación

⁹ Cfr. /PV. 2375, de 6 de junio de 1982, párrs. 23-54.

¹⁰ S/PV. 2611, de 2 de octubre de 1985, párrs. 59 y 64.

¹¹ S/RES/262(1968) de 31 de diciembre.

¹² S/RES/509(1982), de 6 de junio. La Asamblea General, por su parte, calificó la invasión del Líbano de agresión, A/RES-7/5, de 26 de junio de 1982

¹³ S/RES/573(1985) de 4 de octubre.

con el actual régimen regulatorio del uso de la fuerza en el Derecho internacional. En efecto, el artículo 51 de la Carta es una norma primaria que se articula como excepción al principio estructural de la prohibición de la amenaza de uso o del uso de la fuerza (artículo 2.4 CNU). Si bien el derecho de legítima defensa tiene contenido convencional y consuetudinario, como recordó la Corte Internacional de Justicia¹⁴, como excepción, debe ser objeto de interpretación restrictiva siendo el comportamiento deseado que un Estado se abstenga de amenazar con recurrir o de recurrir a la fuerza. Además, los siete requisitos cumulativos que establecen el derecho consuetudinario y el artículo 51 de la Carta para el ejercicio del derecho reafirman dicho carácter restrictivo: i) la existencia de un ataque armado; ii) la atribución de dicho ataque a un Estado; iii) la comunicación al Consejo de Seguridad de las medidas que el Estado víctima del ataque pretende tomar en legítima defensa; iv) la inmediatez de la respuesta en legítima defensa; v) su necesidad; vi) su proporcionalidad tanto en los fines como en los medios; y, vii) su provisionalidad.

Empero, el derecho de legítima defensa ha sido objeto de una interpretación extensiva por parte de ciertos Estados en las últimas décadas con el fin de justificar intervenciones militares bajo el pretexto de ejercer la protección de los nacionales en el extranjero, contra usos indirectos de la fuerza o contra grupos armados no estatales¹⁵, interpretación que no ha sido, por lo general, bien recibida por la comunidad internacional.

¹⁴ *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America)*, Merits, Judgment, ICJ Reports 1986, p. 14, párr. 34. Existe abundante doctrina sobre el análisis por parte de la Corte Internacional de Justicia de las normas relativas al uso de la fuerza, entre otros, JOHN NORTON MOORE, «Jus ad Bellum Before the International Court of Justice», *Virginia Journal of International Law*, vol. 52, 2012, pp. 903-961; JAMES KRASKA, «A Social Justice Theory of Self-Defense at the World Court», *Loyola University Chicago International Law Review*, vol. 9, n° 1, pp. 24-44.

¹⁵ Cfr. RAQUEL REGUEIRO DUBRA, *La legítima defensa en Derecho Internacional*, Instituto Universitario General Gutiérrez Mellado, 2012.

3. El derecho de legítima defensa y la dificultad de la necesaria atribución del ataque armado

La invocación del derecho de legítima defensa contra grupos armados no estatales, calificados de grupos terroristas por parte de ciertos Estados y reconocidos algunos de estos como amenazas al paz y la seguridad internacionales por el Consejo de Seguridad de las Naciones Unidas – como *Al Qaeda* y el Estado Islámico – mostró cierta apertura hacia el argumento de la legalidad del uso de la fuerza para la lucha contra el terrorismo internacional¹⁶, considerando que un ataque terrorista puede calificarse de «ataque armado» en el sentido del artículo 51 de la Carta si, por sus características e intensidad, sería calificado de «ataque armado» en caso de ser llevado a cabo por fuerzas armadas regulares¹⁷. Se excluirían, por lo tanto, del ámbito de aplicación del artículo 2.4 de la Carta y, por ende, de la calificación de «ataque armado» establecida por el artículo 51 de la Carta, aquellos atentados que, por su naturaleza y efectos, no alcancen el umbral mínimo para la activación de las normas relativas al uso de la fuerza¹⁸.

3.1 El «ataque armado» como requisito para el derecho de legítima defensa

El cumplimiento del requisito de «ataque armado» establecido por el artículo 51 de la Carta obliga a atribuir dicho ataque a un Estado. De no ser posible la atribución, no existiría un ataque armado contra el que el Estado pueda articular una respuesta en legítima defensa. En efecto, el derecho de legítima defensa, establecido en un tratado intergubernamental, no deja lugar a dudas: el derecho debe ejercerse por un Estado contra otro. Ello obliga, como señaló en repetidas ocasiones la Corte Internacional de Justicia¹⁹, atribuir el ataque armado a un Estado, lo que, en caso de ataques

¹⁶ Cfr. CHRISTIAN J. TAMS, «The Use of Force against Terrorists», *The European Journal of International Law*, vol. 20, nº 2, 2009, pp. 359-397.

¹⁷ *Military and Paramilitary Activities in and against Nicaragua*, *op. cit.*, párr. 195.

¹⁸ Cfr. TOM RUYTS, «The Meaning of “Force” and the Boundaries of the Jus ad Bellum: Are “Minimal” Uses of Force Excluded from UN Charter Article 2(4)?», *The American Journal of International Law*, vol. 108, nº 2, 2014, pp. 159-210.

¹⁹ Cfr. *Ibid.*, párr. 104; *Oil Platforms (Islamic Republic of Iran v. United States of America)*, *Judgment*, *I.C.J. Reports 2003*, p. 161, párr. 64.

perpetrados por grupos armados no estatales, implica probar la necesaria conexión entre la acción ilícita y el Estado contra el que se dirige la acción defensiva, cuestión harto complicada dado que las normas actuales sobre responsabilidad internacional solo permiten dicha atribución en circunstancias muy específicas y bajo unos requisitos restrictivos, como el requisito del control efectivo o de las instrucciones recibidas (artículo 8 del Proyecto de artículos sobre responsabilidad del Estado por hechos internacionalmente ilícitos), el requisito de buena fe en la violación de una obligación internacional en caso de defecto o ausencia de autoridades oficiales (artículo 9) o el requisito de éxito para la atribución a un Estado de las violaciones del Derecho internacional cometidas por un movimiento insurreccional²⁰.

Estas causas de atribución tienen difícil aplicación a los casos de ataques terroristas realizados por grupos armados no estatales que no guardan una relación directa y estrecha con un Estado. Cabría probar, en efecto, tal grado de implicación del Estado en la planificación, preparación y ejecución del ataque que el grupo armado sería una mera marioneta en sus manos al actuar; como señaló Luis Ignacio Sánchez Rodríguez, «una entidad actuante en nombre y por cuenta [del Estado] en términos de vinculación material reales y operativos»²¹, implicando una suerte de relación orgánica *de facto*²².

Así, siguiendo a Vladyslav Lanovoy, para determinar la condición de órgano *de facto* del grupo, será necesario probar que: i) el actor no estatal ha sido creado por el Estado; ii) la participación del Estado va más allá de provisión de ayuda económica y logística; iii) el Estado tenía pleno control sobre el hecho ilícito; o, iv) el Estado ha seleccionado o pagado a los líderes del grupo²³. En este sentido, las posibilidades de atribución

²⁰ Cfr. igualmente NICHOLAS TSAGOURIAS, «Self-Defense against Non-State Actors: The Interaction between Self-Defense as a Primary Rule and Self-Defense as a Secondary Rule», *Leiden Journal of International Law*, vol. 29, 2016, pp. 801-825.

²¹ LUIS IGNACIO SÁNCHEZ RODRÍGUEZ, *Derecho Internacional y crisis internacionales*, Iustel, Madrid, 2005, p. 200.

²² Cfr. JAN ARNO HESSBRUEGGE, «The Historical Development of the Doctrines of Attribution and Due Diligence in International Law», *New York University Journal of International Law and Politics*, vol. 36, 2004, pp. 265-306.

²³ VLADYSLAV LANOVOY, «The Use of Force by Non-State Actors and the Limits of Attribution of Conduct», *The European Journal of International Law*, vol. 28, n° 2, 2017, pp. 563-585, aquí 575.

no son identificables y claras dado que la participación del Estado no es necesaria para que ocurra el ataque si el Estado no da instrucciones específicas; no apoya de forma decidida al grupo con financiación, entrega de armas u otro apoyo logístico y material hasta el punto que esta ayuda o asistencia suponga un control efectivo del grupo dado que este no podría haber desarrollado de forma exitosa sus actividades sin el apoyo del Estado; o, no consiente de forma clara a ese ataque que parte de su territorio contra otro Estado.

Así la necesidad de la atribución se une a su dificultad, por lo que ciertos Estados²⁴ han propuesto nuevos argumentos, requiriendo una relación más laxa entre el ataque armado y el Estado. Fueron consideradas formas de atribución de un ataque armado el dar cobijo a un grupo terrorista (*Al Qaeda* en Afganistán, 2001), la tolerancia a la presencia de grupos armados en un territorio (*Hezbollah* en el Líbano, 2006) y el hecho que el Estado no quiera o no pueda prevenir atentados terroristas o, en su caso, sancionar a los culpables (*unable/unwilling theory*), restando así cada vez más relevancia a la necesaria existencia de una conexión entre el acto, el autor de dicho acto y el Estado en cuyo territorio tendrá lugar la respuesta en legítima defensa.

En particular, la teoría del Estado «no puede/no quiere» presenta dos escenarios distintos, a menudo confundidos de forma intencionada por parte de los Estados víctima de atentados terroristas²⁵. En el primer caso, el Estado, sabiendo que grupos armados no estatales se encuentran establecidos en su territorio, tiene voluntad de afrontar el problema, pero carece de los medios necesarios para ello. En el segundo caso, el Estado, sabiendo de la presencia de estos grupos en su territorio, no pone fin a su actividad y no permite que terceros Estados lo hagan (no consiente a las actividades armadas de terceros en su territorio). Aún en el caso de que el Estado no quiera, la teoría *unable/unwilling* obliga a determinar de forma clara cuáles son las razones para la negativa de un Estado que, teniendo la capacidad para ello, no afronta el problema de la presencia de un grupo armado no estatal en su territorio. Además, en el marco de la lucha contra

²⁴ Entre ellos, Estados Unidos, el Reino Unido, Rusia, Turquía e Israel.

²⁵ Cfr. THERESA REINOLD, «State Weakness, Irregular Warfare, and the Right to Self-Defense post 9/11», *The American Journal of International Law*, vol. 105, 2011, pp. 244-286.

el Estado Islámico, frente a la imposibilidad de atribuir a Siria los actos terroristas cometidos por el grupo dentro y fuera del territorio bajo su control, algunos Estados afirmaron que el Estado sirio era responsable de dichos ataques porque las autoridades habían incumplido el estándar de conducta requerido, aplicando así el concepto de debida diligencia como forma de atribución de un ataque armado para el ejercicio del derecho de legítima defensa.

3.2 El principio de diligencia debida

Existe consenso en la comunidad internacional respecto de la obligación que tiene todo Estado de prevenir la comisión de ataques armados por parte de grupos armados no estatales desde su territorio hacia otros Estados²⁶. De otra parte, el principio de diligencia debida representa un estándar de comportamiento en las relaciones internacionales que establece una obligación de conducta y no de resultado²⁷, por lo que genera una obligación internacional de carácter objetivo. Así, el elemento subjetivo de conducta de los órganos del Estado puede resultar de utilidad para la atribución de responsabilidad, pero únicamente con fines de prueba para confirmar la violación de la obligación. La Corte Internacional de Justicia afirmó, en su análisis de la posible asistencia proporcionada por Nicaragua a los rebeldes en El Salvador, que sería:

«Clearly unreasonable to demand of the Government of Nicaragua a higher degree of diligence that is achieved by even the combined efforts of the other [...] States. In particular, when Nicaragua is blamed for allowing consignment of arms to cross its territory, this is tantamount, where El Salvador is concerned, to an admission of its inability to stem the flow.»²⁸

²⁶ La Corte Internacional de Justicia señaló en su primera sentencia en un caso contencioso que los Estados no deben permitir el uso de su territorio para la comisión de actos contrarios a los derechos de otros Estados, inclusive aquellos cometidos por individuos; *Corfú Channel case, Judgment of April 9th, 1949, I.C.J. Reports 1949*, p. 4, aquí p. 22.

²⁷ Cfr. *Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v. Serbia and Montenegro), Judgment, I.C.J. Reports 2007*, p. 43, párr. 430.

²⁸ *Military and Paramilitary Activities in and against Nicaragua, op. cit.*, párr. 157.

Así, la Corte estableció, como señala Timo Koivurova²⁹, el grado de diligencia exigible a un Estado en relación con las actividades privadas ilegales que ocurren en su territorio, determinando, en particular, que no resulta exigible el mismo estándar a un Estado con un menor grado de desarrollo que a un Estado desarrollado. Para valorar el cumplimiento del principio, deben tomarse en consideración, *primo*, la efectividad del control ejercido por el Estado sobre su territorio, siendo el Estado requerido de tomar todas las medidas necesarias para asegurar dicha efectividad; *secundo*, la balanza de los intereses que el Estado debe proteger; y, *tertio*, la predictibilidad del daño, tras haber considerado todos los posibles y razonables esfuerzos realizados por el Estado con el fin de obtener suficiente conocimiento respecto de los riesgos y amenazas.

En este sentido, la debida diligencia solo puede aplicarse a obligaciones positivas del Estado (las que consisten en la necesidad de proteger los intereses de terceras partes) y no negativas (aquellas que requieren que el Estado se abstenga de violar los legítimos intereses protegidos de otros Estados). Así, el deber de diligencia no se articula como una forma autónoma de atribución de responsabilidad. En efecto, la debida diligencia requiere que el Estado haga el máximo esfuerzo, dentro de sus capacidades, para prevenir el resultado indeseado.

En este marco, aplica también el principio *ultra posse nemo tenetur* (un Estado no puede ser responsable de actos que escapan a su control). Si el Estado no dispone de medios suficientes (el Estado «no puede») para controlar a los actores privados presentes en su territorio, no puede atribuírsele un incumplimiento de su obligación de diligencia debida³⁰. Por ello, a modo de ejemplo, el mero hecho que una violación internacional tenga lugar en su territorio no es suficiente para establecer *ipso facto* la responsabilidad del Estado respecto de dicho acto. Esto implica que la base para una violación de la obligación de debida diligencia es la conducta misma del Estado y no el acto del actor no estatal, lo que conlleva que, aún en el caso que un Estado

²⁹ TIMO KOIVUROVA, «Due Diligence», in *Max Planck Encyclopedia of International Law*, 2010, párr. 40.

³⁰ Cfr. DAWOOD I. AHMED, «Defending Weak States Against the “Unwilling or Unable” Doctrine of Self-Defense», *Journal of International Law and International Relations*, vol. 9, 2013, pp. 1-37, aquí p. 8.

«pueda y no quiera», su ausencia de participación efectiva en el ataque perpetrado imposibilita la atribución de este³¹.

En un intento de sistematizar la teoría del «no puede/no quiere», Ashley Deeks defiende que el Estado víctima, antes de aplicar la teoría, debe priorizar la obtención del consentimiento y de la cooperación del Estado territorial. Además, resulta esencial evaluar la naturaleza de la amenaza que supone el actor no estatal teniendo en cuenta el ámbito geográfico y la intensidad de sus acciones, el nivel de sofisticación de los ataques perpetrados, el número de miembros del grupo presentes en el territorio, etc. En tercer lugar, el Estado víctima debe solicitar autorización al Estado territorial para responder a dicha amenaza, proponer un marco temporal para realizar su acción y las medidas necesarias para eliminar dicha amenaza, y valorar la capacidad del Estado territorial para abordar de forma exitosa el reto que supone el grupo armado presente en su territorio.³²

No obstante, la sistematización propuesta por Deeks se centra únicamente en la apreciación de la situación por parte del Estado víctima, obviando así el necesario respeto de la soberanía del Estado territorial y cualquier mecanismo de supervisión de la licitud de la acción que deberá recaer forzosamente en el Consejo de Seguridad en el marco de su capacidad de evaluación *ex post facto*. A modo de ejemplo, Estados Unidos no priorizó la obtención del consentimiento de Siria para actuar en su territorio contra el Estado Islámico; de hecho, nunca lo solicitó³³. Por ello, como señala Olivier Corten, la interpretación estadounidense de la teoría «no puede/no quiere» es mucho más extensiva que la propuesta por la doctrina³⁴. Además, no existe *opinio iuris* entre los Estados que apoyan la teoría

³¹ Cfr. *Armed Activities on the Territory of the Congo (Democratic Republic of the Congo v. Uganda)*, Judgment, I.C.J. Reports 2005, p. 168.

³² ASHLEY S. DEEKS, «Unwilling or Unable»: Toward a Normative Framework for Extraterritorial Self-Defense», *Virginia Journal of International Law*, vol. 52, 2012, pp. 483-549, aquí pp. 519-532.

³³ Sobre la intervención militar contra el Estado Islámico y la cuestión del consentimiento, cfr. KARINE BANNELIER-CHRISTAKIS, «Military Interventions against ISIL in Iraq, Syria and Lybia, and the Legal Basis of Consent», *Leiden Journal of International Law*, vol. 29, 2016, pp. 743-775.

³⁴ OLIVIER CORTEN, «The “Unwilling or Unable” Test: Has it Been, and Could it Be, Accepted?», *Leiden Journal of International Law*, vol. 29, 2016, pp. 777-799.

respecto del contenido de esta ni aceptación general de la teoría en la comunidad internacional³⁵.

En efecto, una violación de la obligación de debida diligencia es un incumplimiento en el sentido de los artículos 2 y 12 del Proyecto de artículos sobre responsabilidad del Estado por hechos internacionalmente ilícitos. No obstante, no constituye un ataque armado atribuible al Estado. El Derecho internacional no especifica qué medidas específicas o qué obligaciones precisas implica la obligación general de prevenir actos terroristas. Hasta el deber de cooperación para la prevención de ataques es difusa frente a la obvia necesidad de proteger los intereses y secretos de Estado, así como asegurar la paz a nivel local³⁶.

En otro aparte, la obligación de proteger a los nacionales extranjeros presentes en su territorio no genera, en principio, responsabilidad internacional salvo que, como señala Robert Barnidge, se demuestre que el Estado ha conspirado para ello o falló en su obligación de tomar medidas apropiadas para prevenir daños a extranjeros o si, tras el acontecimiento, las autoridades estatales no realizan un esfuerzo adecuado para hacer justicia.³⁷ Por ello, frente al argumento que defiende que si el Estado no puede o no quiere prevenir dichos actos debe atribuírsele una responsabilidad indirecta (que no contemplan las normas internacionales vigentes)³⁸, cabe refutar que una

³⁵ *Ibidem*. Sobre la relevancia del silencio de ciertos Estados frente a las invocaciones del ejercicio de un derecho de legítima defensa contra actores no estatales, cfr. PAULINA STARKI, «Silence Within the Process of Normative Change and Evolution of the Prohibition on the Use of Force: Normative Volatility and Legislative Responsibility», *Journal on the Use of Force and International Law*, vol. 4, n° 1, pp. 14-65. Cfr. igualmente AGATHA VERDEBOUT, *Rewriting Histories of the Use of Force. The Narrative of "Indifference"*, Cambridge University Press, 2021.

³⁶ Cfr. JOHANNA KULESZA, *Due Diligence in International Law*, Brill Nijhoff, Leiden/Boston, 2016, pp. 159-162.

³⁷ ROBERT P. BARNIDGE, JR., «The Due Diligence Principle Under International Law», *International Community Law Review*, vol. 8, 2006, pp. 81-121. Cfr. igualmente AWALOU OUEDRAOGO, «La due diligence en Droit International: de la règle de la neutralité au principe general», *Revue Générale de Droit International Public*, vol. 42, 2012, pp. 641-683.

³⁸ Cfr., para la argumentación de la necesidad de ajuste de las normas existentes sobre responsabilidad internacional para adecuarlas a las necesidades de la lucha contra el terrorismo, VICENT-JOËL PROULX, «Babysitting Terrorists: Should States Be Strictly Liable for Failing to Prevent Transborder Attacks?», *Berkeley Journal of International Law*, vol. 23, n° 3, 2005, pp. 615-668.

violación de la debida diligencia (aún no queriendo el Estado) signifique un incumplimiento del artículo 2.4 de la Carta (o, en términos del artículo 51, un «ataque armado»)³⁹.

La Corte Internacional de Justicia no consideró el principio de debida diligencia como un concepto de aplicación autónoma, sino que relaciona la existencia de una obligación de diligencia debida del Estado como corolario de una norma primaria⁴⁰. Además, como señala Dawood Ahmed, debido a la (usualmente) enorme disparidad de poder militar entre el Estado del territorio y el Estado víctima de un atentado terrorista:

«In the case of self-defense against non-state actors, there is often low-visibility as to whether or not an armed attack has actually taken place, whether the source is as alleged by the victim state and, most importantly, whether the host state is indeed ineffective at dealing with the suspected perpetrator, as claimed by the victim state. A lack of observability means that it becomes difficult for the international community to detect and therefore punish a victim state that makes arbitrary determinations.»⁴¹

La discusión doctrinal muestra así que la licitud del ejercicio de un derecho de legítima defensa contra actores no estatales presentes en el territorio de otro Estado no es una cuestión pacífica debido a la necesidad de atribución, de acuerdo con las normas vigentes, del comportamiento del grupo al Estado territorial⁴². No obstante, como señala Dire Tladi, «the ar-

³⁹ Cfr. igualmente PAULINA STARSKI, «Right to Self-Defense, Attribution and the Non-State Actor», *ZaöRV*, vol. 75, 2015, pp. 455-501.

⁴⁰ Cfr., entre otros, *Armed Activities on the Territory of the Congo*, *op. cit.*, p. 168, párr. 189; *Application of the Convention on the Prevention and Punishment of the Crime of Genocide*, *op. cit.*, párr. 430. Cfr. igualmente NEIL McDONALD, «The Role of Due Diligence in International Law», *International and Comparative Law Quarterly*, vol. 68, 2019, pp. 1041-1054.

⁴¹ AHMED, *op. cit.*, p. 19

⁴² Para una visión de las posiciones enfrentadas entre la doctrina restrictiva y la doctrina expansionista – con propuestas alternativas, cfr. ANNE PETERS Y CHRISTIAN MARXSEN (eds.), *Self-Defense Against Non-State Actors: Impulses From the Max Planck Dialogues on the Law of Peace and War*, MPIL Research Papers Series, n° 2017-07, Max Planck Institute for Comparative Public Law and International Law. Cfr. igualmente FEDERICA I. PADDEU, «Use of Force against Non-State Actors and the Circumstance Precluding Wrongfulness of Self-Defense», *Leiden Journal of International Law*, vol. 30, 2017, pp. 93-115; TOM RUYSS, «Armed

guments, based on “practice”, that International Law does permit the unilateral use of force against non-state actors on the territory of innocent third states are, at best, unconvincing and, at worst, dangerous»⁴³. En cualquier caso, cabe preguntarse si el argumento de la evolución del derecho de legítima defensa por la práctica de los Estados en relación con su ejercicio frente a actores no estatales se basa en la pretensión de la modificación del régimen normativo relativo al uso de la fuerza o no es más que un intento de interpretación extensiva de la regulación existente⁴⁴.

En este marco, la intervención militar de Israel en el territorio ocupado palestino desde el 7 de octubre de 2023 reta la visión actual de la utilización del uso de la fuerza en el ejercicio de un derecho de legítima defensa frente a actores no estatales. En efecto, el territorio en el que desarrolla la operación militar israelí está bajo ocupación. Por ello, la atribución de los actos terroristas perpetrados por Hamás a un Estado resulta imposible al no existir Estado sino pueblo. Además, el pueblo palestino tiene reconocido el derecho a la libre determinación, derecho humano colectivo absoluto con rango de norma de *ius cogens*. Finalmente, el desarrollo de la operación militar israelí vulnera de forma clara, grave y reiterada las normas relativas a los conflictos armados, en particular en relación con la protección de la población civil, y son numerosas las alegaciones de limpieza étnica e intento de genocidio, invalidando así el argumento – de dudosa aceptación – de la legítima defensa⁴⁵.

Attack” and Article 51 of the UN Charter: Evolutions in Customary Law and Practice, Cambridge University Press, 2010.

⁴³ DIRE TLADI, «The Use of Force in Self-Defense against Non-State Actors, Decline of Collective Security and the Rise of Unilateralism: Whither International Law?», en MARY ELLEN O’CONNELL *et al.*, *Self-Defense against Non-State Actors*, Cambridge University Press, 2019, pp. 14-89, aquí p. 88.

⁴⁴ Cfr. RAPHAËL VAN STEENBERGHE, «The Law of Self-Defense and the New Argumentative Landscape on the Expansionists’ Side», *Leiden Journal of International Law*, vol. 29, 2016, pp. 43-65.

⁴⁵ La aproximación de este estudio se centra en la intervención militar israelí a partir de 7 de octubre de 2023 aunque no es ajena a la doctrina la opinión de que la operación actual no es un uso de la fuerza aislado, sino que constituye una recalificación del uso de la fuerza que ejerció el Estado sobre los territorios palestinos ocupados desde 1967. Cfr. RALPH WILDE, «Israel’s War in Gaza is Not a Valid Act of Self-Defense in International Law», *Opinio Iuris*, disponible en <https://opiniojuris.org/2023/11/09/israels-war-in-gaza-is-not->

4. El caso de la Franja de Gaza: ¿Qué respuesta de fuerza para qué derecho de legítima defensa?

La Corte Internacional de Justicia reconoció tanto en el año 2004 como en el 2024 el derecho a la libre determinación del pueblo palestino⁴⁶ y su anhelo a convertirse en un Estado al declarar que nadie duda – ni siquiera Israel, señala el Tribunal – de la existencia del pueblo palestino⁴⁷ que tiene un territorio, ocupado por Israel desde 1967⁴⁸. En el mismo sentido se pronunció la Asamblea General que señaló que el territorio palestino está bajo ocupación militar, que el pueblo palestino tiene derecho a la libre determinación y a la soberanía respecto de su territorio y que la potencia ocupante, Israel, tiene únicamente los deberes y obligaciones que incumben a una potencia ocupante⁴⁹.

4.1 La Franja de Gaza como territorio palestino ocupado e Israel como potencia ocupante

Si bien el Consejo Nacional de Palestina proclamó la independencia con la Declaración de Argel el 15 de noviembre de 1988 con el apoyo de 114 Estados, Palestina no cumplía en aquel momento, y sigue sin hacerlo a día de hoy, los requisitos para obtener la condición de Estado dado que, a pesar de contar con una población y un territorio y tener la capacidad de establecer relaciones con otros sujetos del Derecho Internacional⁵⁰,

a-valid-act-of-self-defence-in-international-law/ (fecha de última consulta: 12 de febrero de 2024).

⁴⁶ *Legal consequences of the construction of a Wall in the occupied Palestinian territory*, I. C. J. Reports 2004, p. 136, párr. 88; *Legal consequences arising from the policies and practices of Israel in the Occupied Palestinian Territory, including East Jerusalem, Advisory Opinion*, 19 de julio de 2024, párr. 78.

⁴⁷ *Legal consequences of the construction*, *op. cit.*, párrs. 117-118.

⁴⁸ *Ibid.*, párr. 78.

⁴⁹ A/RES/58/292, de 17 de mayo de 2004. La resolución contó con 140 votos a favor, 11 abstenciones y 6 votos en contra (Israel, Islas Marshall, Nauru, Palau, Estados Unidos y Micronesia).

⁵⁰ A nivel regional, Palestina es miembro, entre otros, de la Liga Árabe y de la Organización para la Cooperación Islámica; en el marco universal, tiene condición de Estado miembro de la Corte Penal Internacional y de la UNESCO y de Estado miembro observador en

carece de poder público con control efectivo sobre dicha población y territorio. Sin embargo, no toda creación de un nuevo Estado se fundamenta únicamente en el cumplimiento de estos requisitos, sino que la práctica es mucho más diversa, no siendo infrecuentes los casos de adquisición de la condición de Estado por parte de territorios que carecían de gobierno efectivo⁵¹.

En el caso de Palestina, el control efectivo del territorio se encuentra dividido entre la Autoridad Palestina y Hamás, que controla la Franja de Gaza desde su victoria en las elecciones legislativas del año 2006, un resultado que se negaron a reconocer tanto Estados Unidos, como la propia Israel y la Unión Europea. Desde ese momento, todos los intentos de Al Fatah y Hamás de crear un gobierno de unidad han fracasado. Así, Hamás mantiene un concepto de lucha armada contra Israel que combina con su función de gobierno *de facto* en Gaza. Israel considera, desde su desconexión de Gaza del año 2005, que la Franja no es un territorio ocupado ni controlado por Israel. La Corte Internacional de Justicia determinó que un territorio se considera ocupado cuando se encuentra efectivamente bajo la autoridad del ejército enemigo y que la ocupación solo se extiende a aquellos territorios en los que dicha autoridad está establecida y puede ser ejercida⁵².

Ahora bien, la afirmación israelí resulta poco creíble cuando el bloqueo israelí de la Franja de Gaza implica que Israel no solo controla el movimiento de la población y de los productos de Gaza, sino que igualmente interviene la única frontera operativa entre la Franja y Egipto, el paso de *Rafah*⁵³. La

la Asamblea General de las Naciones Unidas (A/RES/67/19, de 4 de diciembre de 2012).

⁵¹ Una situación común durante el proceso de descolonización fue el reconocimiento por parte de la comunidad internacional, y en particular la aceptación de la adhesión a la Carta de las Naciones Unidas, de nuevos Estados que carecían de un gobierno efectivo, como en el caso de la República Democrática del Congo, Ruanda o Burundi.

⁵² *Legal consequences of the construction of a Wall in the occupied Palestinian territory*, *op. cit.*, párr. 78.

⁵³ Agreement on Movement and Access (AMA), de 15 de noviembre de 2005, disponible en <https://www.eubam-rafah.eu/sites/default/files/u173/Agreement%20on%20Movement%20and%20Access.pdf> (fecha de última consulta: 11 de febrero de 2024). Cfr. igualmente Agreed Principles for Rafah Crossing (APRC), que muestran el nivel de control israelí en relación con el paso, disponible en [https://www.eubam-rafah.eu/sites/default/files/u173/Agreed%](https://www.eubam-rafah.eu/sites/default/files/u173/Agreed%20Principles%20for%20Rafah%20Crossing.pdf)

existencia de la ocupación israelí en Gaza ha sido ampliamente reconocida en el ámbito internacional. Así, la Comisión Económica y Social para Asia divide a los palestinos que viven directamente bajo dominio israelí en tres categorías: 1) aquellos que son ciudadanos de Israel; 2) aquellos que residen en Jerusalén Este; y, 3) aquellos que viven bajo ocupación en Cisjordania y Gaza⁵⁴ y añade:

«Israel military law continues to apply for Gaza regarding exclusive Israeli control over Palestinian movement and trade in and out of the territory, the unilaterally imposed “security zone” along the perimeter fence, and Palestinian access to fishing areas and sea routes. Gaza remains, therefore, under military occupation in the eyes of the United Nations.»⁵⁵

En el mismo sentido, la ocupación de la Franja de Gaza por parte de Israel a pesar de su desconexión en el año 2005 encuentra eco en la posición de los Estados en el Consejo de Seguridad⁵⁶; en las resoluciones de este órgano⁵⁷; es reiterada en el Informe Goldstone⁵⁸; y, es apoyada por la doctrina científica⁵⁹. Terry Gill remarca que:

20Principles%20for%20Rafah%20Crossing.pdf (fecha de última consulta: 11 de febrero de 2024).

⁵⁴ Israeli Practices towards the Palestinian People and the Question of Apartheid. Palestine and the Israeli Occupation, Issue no. 1, Economic and Social Commission for Western Asia, United Nations, Doc. E/ESCWA/ECRI/2017/1, 2017, p. 27. Cfr. igualmente Israeli settlements in the Occupied Palestinian Territory, including East Jerusalem, and the Occupied Syrian Golan. Report of the Secretary-General, Doc. A/78/554, de 25 de octubre de 2023.

⁵⁵ *Ibid.*, p. 44. Cfr. igualmente AEYAL GROSS, *The Writing on the Wall. Rethinking the International Law of Occupation*, Cambridge University Press, 2017, pp. 136-264.

⁵⁶ Cfr., a modo de ejemplo, S/PV. 6060, de 31 de diciembre de 2008.

⁵⁷ Cfr., entre otras, S/RES/2334, de 23 de diciembre de 2016, en la que el Consejo reitera que no reconocerá ningún cambio a las líneas del 4 de junio de 1967 que no sean los acordados por las partes mediante negociaciones, y la reciente resolución S/RES/2720, de 22 de diciembre de 2023, en la que el Consejo destaca que «la Franja de Gaza constituye una parte integral del territorio ocupado en 1967».

⁵⁸ Informe de la Misión de Investigación de las Naciones Unidas sobre el Conflicto de Gaza, Doc. A/HRC/12/48, de 25 de septiembre de 2009.

⁵⁹ Cfr. CHRISTIAN HENDERSON, «Israeli Military Operations Against Gaza: Operation Cast Lead (2008-09), Operation Pillar Of Defence (2012), and Operation Protective Edge (2014)», en TOM RUYS y OLIVIER CORTEN (eds.), *The Use of Force in International Law. A*

La debida diligencia y el derecho de legítima defensa frente al terrorismo...

«Israel maintains effective control over Gaza by virtue of its control over Gazan airspace and territorial waters, its control over all but one of the entry points into Gaza, its control over the supply of electricity and other basic amenities to the territory and its general military and technological superiority.»⁶⁰

Por su parte, Alain Bockel añade:

«L'exercice d'un contrôle extérieur sur les frontières impose à la puissance qui l'exerce le respect des droits des populations civiles résidant à leur intérieur. Ce contrôle est [...] total. [...] En fermant la totalité des autres issues [*frontières*], [Israel] conserve le contrôle, certes indirect, mais effectif de ce passage.»⁶¹

El control efectivo de Israel sobre la Franja de Gaza fue puesto de manifiesto cuando el Estado decidió establecer un estado de sitio en la Franja sometiendo así a la población palestina a un castigo colectivo⁶².

4.2 La inexistencia del derecho de legítima defensa de la potencia ocupante en un territorio ocupado

Partiendo de que la Franja de Gaza forma parte integrante del territorio palestino ocupado, la invocación del derecho de legítima defensa por parte

Case-based Approach, Oxford University Press, 2018, pp. 729-748; CHANTAL MELONI y GIANNI TOGNONI (eds.), *Is There a Court for Gaza? A Test Bench for International Justice*, Springer, 2012, pp. 20-21; ORNA BEN-NAFTALI, AEYAL M. GROOS y KEREN MICHAELI, «Illegal Occupation: Framing the Occupied Palestinian Territory», *Berkeley Journal of International Law*, vol. 23, n° 3, 2005, pp. 551-614.

⁶⁰ TERRY GILL, «The ICJ Wall Advisory Opinion and Israel's Right of Self-Defense in Relation to the Current Armed Conflict in Gaza», *Armed Groups and International Law*, 13 de noviembre de 2023, disponible en <https://www.armedgroups-internationallaw.org/2023/11/13/the-icj-wall-advisory-opinion-and-israels-right-of-self-defence-in-relation-to-the-current-armed-conflict-in-gaza/> (última consulta: 12 de febrero de 2024).

⁶¹ ALAIN BOCKEL, «Gaza: le processus de paix en question», *Annuaire Français de Droit International*, vol. 55, 2009, pp. 173-187.

⁶² Cfr. S/PV. 9462, de 30 de octubre de 2023, en la que el Comisionado General de la UNRWA calificó las acciones israelíes de *castigo colectivo* contra la población civil; en el mismo sentido, Secretary General's statement to the press – On the Middle East, de 15 de enero de 2024; Gaza: Report from the Ground, Office of the High Commissioner for Human Rights, Press Briefing Notes, de 19 de enero de 2024.

de Israel solo puede justificar una violación del artículo 2.4 de la Carta por parte de Palestina, circunstancia que resulta imposible dado que ello exige que Palestina sea un Estado. Cualquier argumento de un posible reconocimiento implícito por parte de Israel de Palestina como sujeto pleno del Derecho internacional es vano dado que la posición oficial de Israel respecto del futuro estatus de Palestina va ciertamente en el sentido contrario, negando las autoridades israelíes la posibilidad de un futuro Estado palestino⁶³. Además, aceptar que Israel considera Palestina un Estado para el ejercicio del derecho de legítima defensa, pero le niega dicha condición para todo lo demás, implicaría una perversión de las normas internacionales que no tiene cabida en el Derecho internacional y obligaría a aceptar que Israel pueda beneficiarse de su injusto.

En segundo lugar, como señala Marko Milanovic⁶⁴, el artículo 2.4 de la Carta no es aplicable a situaciones en las que Israel usa la fuerza contra Hamás, como tampoco lo es cuando Hamás recurre a la fuerza contra Israel, por lo que, si la prohibición no aplica, su excepción (la legítima defensa) tampoco. En efecto, la naturaleza de territorio ocupado del territorio palestino invalida *per se* el argumento del derecho de legítima defensa, como había recordado la Corte Internacional de Justicia en el año 2004:

«Article 51 of the Charter thus recognizes the existence of an inherent right of self-defense in the case of armed attack by one State against another State. However, Israel does not claim that the attacks against it are imputable to a foreign State. The Court also notes that Israel exercises control in the Occupied Palestinian Territory and that, as Israel itself states, the threat [...] originates within, and not outside, that territory.»⁶⁵

Así, estando el actor no estatal presente en el territorio que controla y ocupa Israel y habiendo partido la operación «Inundación de al-Aqsa»

⁶³ El Secretario General de las Naciones Unidas y numerosos Estados reaccionaron de forma tajante al anuncio israelí, cfr. S/PV. 9534, de 23 y 24 de enero de 2024.

⁶⁴ MARKO MILANOVIC, «Does Israel Have the Right to Defend Itself?», *EJIL: Talk!*, 14 de noviembre de 2023, disponible en <https://www.ejiltalk.org/does-israel-have-the-right-to-defend-itself/> (fecha de última consulta: 12 de febrero de 2024).

⁶⁵ *Legal consequences of the construction of a Wall in the occupied Palestinian territory*, *op. cit.*, párr. 139.

de dicho territorio, no cabe el derecho de legítima defensa puesto que el ataque armado no tiene carácter internacional al no ser atribuible a un Estado extranjero.

Israel insistió, sin embargo, en la idea de que Hamás representa al pueblo palestino, como manifestó su representante en el Consejo de Seguridad:

«I will begin by saying that if Hamas does not represent the Palestinian people, as President Abbas stated just yesterday, it is puzzling that his representative is present in this meeting, let alone voicing an opinion on behalf of the people in Gaza who elected the Islamic State in Iraq and the Sham (ISIS)-like Hamas murderers in Gaza 17 years ago.»⁶⁶

El representante internacionalmente reconocido del pueblo palestino es la Autoridad Palestina y no Hamás. Ciertamente, el grupo armado no es un movimiento insurreccional en el sentido del artículo 10 del Proyecto de artículos sobre responsabilidad del Estado por hechos internacionalmente ilícitos, por lo que, aún siendo hipotéticamente declarada la condición de Estado de Palestina, las acciones de Hamás no conllevarían responsabilidad internacional del nuevo Estado. Por otra parte, el derecho a la resistencia armada por parte del pueblo palestino solo podrá ser ejercido por el propio pueblo o por sus representantes, en los cuales no está Hamás.

4.3 La inoperatividad de la obligación de diligencia debida para la determinación de un incumplimiento del principio de la prohibición del uso de la fuerza

¿Podría, entonces, Israel argumentar que la Autoridad Palestina falló en su deber de diligencia debida al haber permitido que Hamás utilizase el territorio ocupado para lanzar acciones de fuerza armada contra la potencia ocupante? En otras palabras, ¿aplica el principio de debida diligencia a los movimientos de liberación nacional?

Como señala Andrew Clapham,

“Los rebeldes (insurgentes no reconocidos) como destinatarios de las obligaciones internacionales bajo el derecho internacional humanitario

⁶⁶ S/PV. 9439, *op. cit.*, p. 10.

contemporáneo, especialmente las obligaciones que figuran en el artículo 3 común a los cuatro Convenios de Ginebra de 1949, el Protocolo II de 1977 adicional a los Convenios de Ginebra y el artículo 19 de la Convención de La Haya sobre los bienes culturales, de 1954. [...] Hoy en día, el derecho internacional impone obligaciones a ciertas partes en un conflicto armado interno independientemente del reconocimiento efectuado por el Estado contra el cual están combatiendo o por un tercer Estado. El problema es que los Gobiernos por lo general son reticentes a admitir que se reúnen las condiciones para la aplicación del derecho internacional, ya que aceptar tal situación equivaldría a reconocer que el Gobierno ha perdido cierto grado de control y a “elear” el estatuto de los rebeldes.”⁶⁷

Si los rebeldes no reconocidos están sujetos a obligaciones internacionales, no cabe duda de que los movimientos de liberación nacional también, en particular a las obligaciones del Derecho internacional humanitario, aún en ausencia de control del territorio o de un reconocimiento expreso por parte de la Potencia ocupante.

Si bien la situación en Gaza no se puede calificar de una guerra de liberación nacional en el sentido del artículo 1.4 del Protocolo adicional I a los Convenios de Ginebra de 1949 al no haber ratificado Israel el Protocolo adicional y no ser Hamás parte del movimiento de liberación nacional, el conflicto es un conflicto armado no internacional en el contexto del cual aplican las normas de DIH pertinentes, en particular el artículo 3 común a las 4 Convenios de Ginebra y el IV Convenio relativo a la protección debida a las personas civiles en tiempos de guerra⁶⁸. En este sentido se pronunció la Corte Internacional de Justicia en su opinión consultiva del año 2004:

⁶⁷ ANDREW CLAPHAM, «Obligaciones dimanantes de los derechos humanos para los actores no estatales en situaciones de conflicto», *International Review of the Red Cross*, n° 863, 2006.

⁶⁸ Cfr. igualmente JÉRÔME DE HEMPTINNE, «Classifying the Gaza Conflict Under International Humanitarian Law, a Complicated Matter», *EJIL: Talk!*, 13 de noviembre de 2023, disponible en <https://www.ejiltalk.org/classifying-the-gaza-conflict-under-international-humanitarian-law-a-complicated-matter/> (fecha de última consulta: 12 de febrero de 2024); PETER MAURER, «Challenges to International Humanitarian Law: Israel’s Occupation Policy», *International Review of the Red Cross*, vol. 94, n° 88, 2012. La Corte Internacional reafirmó la aplicación del IV Convenio de Ginebra a los territorios palestinos ocupados en su opinión consultiva del año 2004: *Legal consequences of the construction of a Wall in the occupied Palestinian territory*, *op. cit.*, párr. 101

“The Court accordingly finds that that Convention is applicable in the Palestinian territories which before the conflict lay to the east of the Green Line and which, during that conflict, were occupied by Israel, there being no need for any enquiry into the precise prior status of those territories.”

Con anterioridad, la Corte ya había determinado que:

“It is undoubtedly because a great many rules of humanitarian law applicable in armed conflict are so fundamental to the respect of the human person and “elementary considerations of humanity” as the Court put it in its Judgment of 9 April 1949 in the *Corfu Channel* case (I.C.J. Reports 1949, p. 22), that the Hague and Geneva Conventions have enjoyed a broad accession. Further these fundamental rules are to be observed by all States whether or not they have ratified the conventions that contain them, because they constitute intransgressible principles of international customary law.”⁶⁹

El Comité Internacional de la Cruz Roja reconoce igualmente que el DIH aplica a aquellos que han cometido actos terroristas, sean estos las fuerzas armadas regulares del Estado, movimientos de liberación nacional, otros movimientos de resistencia, miembros disidentes de las fuerzas armadas involucrados en un conflicto armado interno o grupos que pueden ser considerados como grupos terroristas al consistir su actividad principal la ejecución de atentados terroristas⁷⁰.

Ahora bien, la existencia de obligaciones internacionales a cargo del movimiento de liberación nacional no implica un deber de diligencia debida. En efecto, el movimiento solo podrá prevenir aquellos actos respecto de los cuales mantenga cierto control. La Autoridad Palestina no tiene control sobre Hamás y ni la propia Israel alegó la participación de *Fatah* en los actos de 7 de octubre centrando la responsabilidad de dichos actos en Hamás. Aún en la interpretación más extensiva del deber de diligencia debida en el marco de una posible discusión de Palestina como Estado, cabría demostrar

⁶⁹ *Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, I.C.J. Reports 1996*, p. 226, párr. 79.

⁷⁰ Fundamentals of IHL en How does Law Protect in War?, International Committee of the Red Cross, disponible en https://casebook.icrc.org/law/fundamentals-ihl#2-3-b_bb (fecha de última consulta: 12 de febrero de 2024).

que, pudiendo hacerlo, la Autoridad Palestina (su gobierno) no quiso prevenir la operación «Inundación de al-Aqsa» y valorar las razones para su negativa, estableciendo así la responsabilidad internacional de Palestina por la comisión de un hecho ilícito internacional pero no de un «ataque armado» en el sentido del artículo 51 de la Carta.

4.4 La proporcionalidad como requisito confirmatorio de medidas armadas sin fines defensivos

Si bien no cabe aceptar la invocación del derecho de legítima defensa de Israel para la justificación de sus acciones armadas en territorio palestino, inclusive Gaza, este análisis no puede ignorar que, aún aceptando la posición israelí de que el derecho de legítima defensa aplica en este caso, el flagrante incumplimiento por parte de Israel del requisito consuetudinario de proporcionalidad de la acción militar invalidaría *per se* cualquier argumento de justificación de la intervención. En este contexto, cabe diferenciar de forma clara el requisito de proporcionalidad del derecho de legítima defensa y el principio de proporcionalidad que aplica en el marco del *ius in bello*⁷¹. Así, el derecho aplicable a los conflictos armados no depende de la licitud de la acción que inició dicho conflicto (*ius ad bellum*)⁷². No obstante, las violaciones graves y reiteradas del Derecho internacional humanitario en el marco de una acción alegada como defensiva permiten valorar la necesidad de dicha acción, así como su proporcionalidad.

En este sentido, en cualquiera de las vertientes de la proporcionalidad en el marco del ejercicio de un derecho de legítima defensa, la acción israelí incumple el requisito. Respecto de la proporcionalidad en los medios, la acción defensiva llevada a cabo debe ser proporcionada a la naturaleza e

⁷¹ Sobre la proporcionalidad en marco del *ius in bello*, cfr. JAMES KILCUP, «Proportionality in Customary International Law: An Argument Against Aspirational Laws of War», *Chicago Journal of International Law*, vol. 17, nº 1, 2016, pp. 244-272; JEREMY RABKIN, «Proportionality in Perspective: Historical Light on the Law of Armed Conflict», *San Diego International Law Journal*, vol. 16, 2015, pp. 263-340.

⁷² Cfr. KEIICHIRO OKIMITO, «The Cumulative Requirements of Jus ad Bellum and Jus in Bello in the Context of Self-Defense», *Chinese Journal of International Law*, 2012, pp. 45-75.

intensidad del ataque sufrido y suficiente para desactivarlo.⁷³ En el caso objeto de nuestro estudio, el número de víctimas palestinas, la intensidad de los bombardeos israelíes, la rudeza de las intervenciones en terreno y, en general, el nivel de destrucción provocado por Israel en (aunque no solo) la Franja de Gaza, muestra una clara desproporción de la fuerza armada en relación con la operación *Inundación de al-Aqsa*. Respecto de la proporcionalidad en los fines, que valora la adecuación de la respuesta armada a tenor de los objetivos de esta, las alegaciones israelíes de que el uso de la fuerza es necesario para destruir la capacidad de Hamás de atacar a Israel en el futuro encuentra igualmente resistencia en la comunidad internacional. Aquí resulta de relevancia, como señala Raphael Van Steenberghe, el uso del «test de desproporcionalidad»:

“Manifest (or gross) disproportion’ test involved by the condition of proportionality seems to be used by States not in order to make cynical calculations, but to assess whether the condition of necessity is fulfilled. [...] The manifestly disproportionate nature of the damage caused by the action in self-defense, compared to the damage caused by the armed attack, is actually used by State as an easy means for ascertaining the unnecessary nature of the measure taken in self-defense. This allows State determining that the action in self-defense is pursuing another (unlawful) purpose that the defense of the victim State, such as retribution or revenge.”⁷⁴

En el mismo sentido, Adil Ahmad Haque, sostiene que es tanta la desproporcionalidad entre el daño que genera la acción israelí y el daño que pretende evitar dicha acción que aquella no cumple con el requisito. Además, defiende que el objetivo de destrucción de Hamás no es un propósito defensivo, dado que los Estados solo tienen derecho (en legítima defensa) de parar o repeler un ataque armado en curso y prevenir uno

⁷³ REGUEIRO DUBRA, *op. cit.*, p. 105.

⁷⁴ RAPHAEL VAN STEENBERGHE, «A Plea for a Right of Israel to Self-Defence in Order to Restrict its Military Operations in Gaza: When Ius ad Bellum Comes to the Aid of Ius in Bello», *Ejil: Talk!*, de 16 de noviembre de 2023, disponible en <https://www.ejiltalk.org/a-plea-for-a-right-of-israel-to-self-defence-in-order-to-restrict-its-military-operations-in-gaza-when-jus-ad-bellum-comes-to-the-aid-of-jus-in-bello/> (fecha de última consulta: 12 de febrero de 2024).

inminente⁷⁵ (excluyendo así la posibilidad del ejercicio preventivo de la legítima defensa en línea con la jurisprudencia de la Corte Internacional de Justicia).⁷⁶

La acción militar israelí en la Franja de Gaza es objeto del contencioso entre Sudáfrica e Israel ante la Corte Internacional de Justicia. Israel alegó expresamente ante el Tribunal que sus operaciones militares en la Franja están justificadas por el ejercicio de un derecho de legítima defensa⁷⁷ frente al argumento de Sudáfrica que considera que las acciones militares de Israel constituyen un delito de genocidio en el sentido de la Convención para la prevención y la sanción del delito de genocidio de 1948. Las órdenes de medidas provisionales dictadas por la Corte⁷⁸ dejan irresuelta, de momento, su valoración en relación con la licitud de un derecho de legítima defensa, tanto en cuanto al principio (la posibilidad de ejercicio de la legítima defensa contra Hamás) como a su ejecución (los requisitos de necesidad y proporcionalidad).

5. Reflexiones finales

La operación militar israelí en el territorio palestino ocupados no encuentra acomodo en las normas relativas al uso de la fuerza establecidas por la Carta de las Naciones Unidas. El argumento del ejercicio de un derecho de legítima defensa frente a los ataques terroristas perpetrados por Hamás desde la Franja de Gaza es vano dado que la operación «Espadas de

⁷⁵ ADIL AHMAD HAQUE, «Enough: Self-Defense and Proportionality in the Israel-Hamas Conflict», *Just Security*, 6 de noviembre de 2023, disponible en <https://www.justsecurity.org/89960/enough-self-defense-and-proportionality-in-the-israel-hamas-conflict/> (fecha de última consulta: 12 de febrero de 2024).

⁷⁶ Cfr. *Military and Paramilitary Activities in and against Nicaragua*, *op. cit.*, párr. 195; *Oil Platforms*, *op. cit.*, párr. 51.

⁷⁷ Public sitting held on Friday 12 January 2024 in the case concerning *Application of the Convention on the prevention and punishment of the crime of genocide in the Gaza Strip (South Africa v. Israel)*, Verbatim Record, International Court of Justice, CR 2024/2.

⁷⁸ *Application of the Convention on the Prevention and Punishment of the Crime of Genocide in the Gaza Strip (South Africa v. Israel)*, Order, 24 de enero de 2024; *Application of the Convention on the prevention and punishment of the crime of genocide in the Gaza Strip (South Africa v. Israel)*, Order, 28 de marzo de 2024; *Application of the Convention on the prevention and punishment of the crime of genocide in the Gaza Strip (South Africa v. Israel)*, Order, 28 de mayo de 2024.

Hierro» no cumple el requisito esencial de la existencia de un ataque armado atribuible a un Estado como violación del principio de la prohibición de uso de la fuerza, por lo que no se articula un derecho de legítima defensa de la potencia ocupante en un territorio que ocupa. El principio de diligencia debida es igualmente inoperativo en este contexto al no construirse como una causa de atribución de un hecho ilícito. Si bien el principio formula una obligación internacional, el incumplimiento de dicho deber tampoco constituye un «ataque armado». En este contexto, la operación militar israelí en Gaza marca nuevos límites de la invocación del derecho de legítima defensa frente al terrorismo internacional en territorios ocupados.

Bibliografía

- AHMAD HAQUE, ADIL, «Enough: Self-Defense and Proportionality in the Israel-Hamas Conflict», *Just Security*, 6 de noviembre de 2023, disponible en <https://www.justsecurity.org/89960/enough-self-defense-and-proportionality-in-the-israel-hamas-conflict/>
- AHMED, DAWOOD I, «Defending Weak States Against the “Unwilling or Unable” Doctrine of Self-Defense», *Journal of International Law and International Relations*, vol. 9, 2013, pp. 1-37
- BANNELIER-CHRISTAKIS, KARINE, «Military Interventions against ISIL in Iraq, Syria and Lybia, and the Legal Basis of Consent», *Leiden Journal of International Law*, vol. 29, 2016, pp. 743-775
- CORTEN, OLIVIER, «The “Unwilling or Unable” Test: Has it Been, and Could it Be, Accepted?», *Leiden Journal of International Law*, vol. 29, 2016, pp. 777-799
- BARNIDGE, JR., ROBERT P., «The Due Diligence Principle Under International Law», *International Community Law Review*, vol. 8, 2006, pp. 81-121
- BEN-NAFTALI, ORNA, GROOS, AEYAL M. y MICHAELI, KEREN, «Illegal Occupation: Framing the Occupied Palestinian Territory», *Berkeley Journal of International Law*, vol. 23, nº 3, 2005, pp. 551-614
- BOCKEL, ALAIN, «Gaza: le processus de paix en question», *Annuaire Français de Droit International*, vol. 55, 2009, pp. 173-187
- BOSCO, DAVID, «Letters from the Front Lines: State Communications to the U.N. Security Council During Conflict», *Columbia Journal of Transnational Law*, vol. 54, 2016, pp. 341-381

- CLAPHAM, ANDREW, «Obligaciones dimanantes de los derechos humanos para los actores no estatales en situaciones de conflicto», *International Review of the Red Cross*, nº 863, 2006
- DEEKS, ASHLEY S., «“Unwilling or Unable”: Toward a Normative Framework for Extraterritorial Self-Defense», *Virginia Journal of International Law*, vol. 52, 2012, pp. 483-549
- GARCÍA-CALVO, CAROLA y VICENTE, ÁLVARO, «La operación “Inundación de al-Aqsa” de Hamás y sus repercusiones en el yihadismo global», *ARI*, 101/2023, pp. 1-7
- GILL, TERRY, «The ICJ Wall Advisory Opinion and Israel’s Right of Self-Defense in Relation to the Current Armed Conflict in Gaza», in *Armed Groups and International Law*, 13 de noviembre de 2023, disponible en <https://www.armedgroups-internationallaw.org/2023/11/13/the-icj-wall-advisory-opinion-and-israels-right-of-self-defence-in-relation-to-the-current-armed-conflict-in-gaza/>
- GREEN, JAMES A., «The Article 51 Reporting Requirement of Self-Defense Actions», *Virginia Journal of International Law*, vol. 55, nº 3, pp. 563-624
- GROSS, AEYAL, *The Writing on the Wall. Rethinking the International Law of Occupation*, Cambridge University Press, 2017, pp. 136-264
- HEMPTINNE, JÉRÔME DE, «Classifying the Gaza Conflict Under International Humanitarian Law, a Complicated Matter», *EJIL: Talk!*, 13 de noviembre de 2023, disponible en <https://www.ejiltalk.org/classifying-the-gaza-conflict-under-international-humanitarian-law-a-complicated-matter/>
- HENDERSON, CHRISTIAN, «Israeli Military Operations Against Gaza: Operation Cast Lead (2008-09), Operation Pillar Of Defence (2012), and Operation Protective Edge (2014)», en TOM RUYS y OLIVIER CORTEN (eds.), *The Use of Force in International Law. A Case-based Approach*, Oxford University Press, 2018, pp. 729-748
- HESSBRUEGGE, JAN ARNO, «The Historical Development of the Doctrines of Attribution and Due Diligence in International Law», *New York University Journal of International Law and Politics*, vol. 36, 2004, pp. 265-306
- KILCUP, JAMES, «Proportionality in Customary International Law: An Argument Against Aspirational Laws of War», *Chicago Journal of International Law*, vol. 17, nº 1, 2016, pp. 244-272
- KOIVUROVA, TIMO, «Due Diligence», in *Max Planck Encyclopedia of International Law*, 2010

- KRASKA, JAMES, «A Social Justice Theory of Self-Defense at the World Court», *Loyola University Chicago International Law Review*, vol. 9, nº 1, pp. 24-44
- KULESZA, JOHANNA, *Due Diligence in International Law*, Brill Nijhoff, Leiden/Boston, 2016
- LANOVOY, VLADYSLAV, «The Use of Force by Non-State Actors and the Limits of Attribution of Conduct», *European Journal of International Law*, vol. 28, nº 2, 2017, pp. 563-585
- MAURER, PETER, «Challenges to International Humanitarian Law: Israel's Occupation Policy», *International Review of the Red Cross*, vol. 94, nº 88, 2012
- MCDONALD, NEIL, «The Role of Due Diligence in International Law», *International and Comparative Law Quarterly*, vol. 68, 2019, pp. 1041-1054
- MELONI, CHANTAL y TOGNONI, GIANNI (eds.), *Is There a Court for Gaza? A Test Bench for International Justice*, Springer, 2012
- MILANOVIC, MARKO, «Does Israel Have the Right to Defend Itself?», *EJIL: Talk!*, 14 de noviembre de 2023, disponible en <https://www.ejiltalk.org/does-israel-have-the-right-to-defend-itself/>.
- MOORE, JOHN NORTON, «*Jus ad Bellum* Before the International Court of Justice», *Virginia Journal of International Law*, vol. 52, 2012, pp. 903-961
- OKIMITO, KEIICHIRO, «The Cumulative Requirements of *Jus ad Bellum* and *Jus in Bello* in the Context of Self-Defense», *Chinese Journal of International Law*, 2012, pp. 45-75
- OUEDRAOGO, AWALOU, «La due diligence en Droit International: de la règle de la neutralité au principe general», *Revue Générale de Droit International Public*, vol. 42, 2012, pp. 641-683
- PADDEU, FEDERICA I., «Use of Force against Non-State Actors and the Circumstance Precluding Wrongfulness of Self-Defense», *Leiden Journal of International Law*, vol. 30, 2017, pp. 93-115
- PETERS, ANNE Y MARXSEN, CHRISTIAN (eds.), *Self-Defense Against Non-State Actors: Impulses From the Max Planck Trialogues on the Law of Peace and War*, MPIL Research Papers Series, nº 2017-07, Max Planck Institute for Comparative Public Law and International Law
- PROULX, VICENT-JOËL, «Babysitting Terrorists: Should States Be Strictly Liable for Failing to Prevent Transborder Attacks?», *Berkeley Journal of International Law*, vol. 23, nº 3, 2005, pp. 615-668

- RABKIN, JEREMY, «Proportionality in Perspective: Historical Light on the Law of Armed Conflict», *San Diego International Law Journal*, vol. 16, 2015, pp. 263-340
- REGUEIRO DUBRA, RAQUEL, *La legítima defensa en Derecho Internacional*, Instituto Universitario General Gutiérrez Mellado, 2012
- REINOLD, THERESA, «State Weakness, Irregular Warfare, and the Right to Self-Defense post 9/11», *American Journal of International Law*, vol. 105, 2011, 244-286
- RUYS, TOM, «*Armed Attack*» and Article 51 of the UN Charter: Evolutions in Customary Law and Practice, Cambridge University Press, 2010
- RUYS, TOM, «The Meaning of “Force” and the Boundaries of the Jus ad Bellum: Are “Minimal” Uses of Force Excluded from UN Charter Article 2(4)?», *American Journal of International Law*, vol. 108, n° 2, 2014, pp. 159-210
- SÁNCHEZ RODRÍGUEZ, LUIS IGNACIO, *Derecho Internacional y crisis internacionales*, Iustel, Madrid, 2005
- STARSKI, PAULINA, «Right to Self-Defense, Attribution and the Non-State Actor», *ZaöRV*, vol. 75, 2015, pp. 455-501
- STARSKI, PAULINA, «Silence Within the Process of Normative Change and Evolution of the Prohibition on the Use of Force: Normative Volatility and Legislative Responsibility», *Journal on the Use of Force and International Law*, vol. 4, n° 1, pp. 14-65
- TAMS, CHRISTIAN J, «The Use of Force against Terrorists», *European Journal of International Law*, vol. 20, n° 2, 2009, pp. 359-397
- TLADI, DIRE, «The Use of Force in Self-Defense against Non-State Actors, Decline of Collective Security and the Rise of Unilateralism: Whither International Law?», en MARY ELLEN O’CONNELL *et al.*, *Self-Defense against Non-State Actors*, Cambridge University Press, 2019, pp. 14-89
- TSAGOURIAS, NICHOLAS, «Self-Defense against Non-State Actors: The Interaction between Self-Defense as a Primary Rule and Self-Defense as a Secondary Rule», *Leiden Journal of International Law*, vol. 29, 2016, pp. 801-825
- VAN STEENBERGHE, RAPHAEL, «A Plea for a Right of Israel to Self-Defence in Order to Restrict its Military Operations in Gaza: When Ius ad Bellum Comes to the Aid of Ius in Bello», *Ejil: Talk!*, de 16 de noviembre de 2023, disponible en <https://www.ejiltalk.org/a-plea-for-a-right-of->

israel-to-self-defence-in-order-to-restrict-its-military-operations-in-gaza-when-jus-ad-bellum-comes-to-the-aid-of-jus-in-bello/

VAN STEENBERGHE, RAPHAËL, «The Law of Self-Defense and the New Argumentative Landscape on the Expansionists' Side», *Leiden Journal of International Law*, vol. 29, 2016, pp. 43-65

VERDEBOUT, AGATHA, *Rewriting Histories of the Use of Force. The Narrative of "Indifference"*, Cambridge University Press, 2021

WILDE, RALPH , «Israel's War in Gaza is Not a Valid Act of Self-Defense in International Law», *Opinio Iuris*, disponible en <https://opiniojuris.org/2023/11/09/israels-war-in-gaza-is-not-a-valid-act-of-self-defence-in-international-law/>

Um olhar sobre o eco-terrorismo. Breves contributos para o Direito Internacional*

Shedding light on eco-terrorism. Brief contributions to International Law

Ricardo Rodrigues de Oliveira

Resumo: Em Março de 2019, o Paquistão anunciou a intenção de formalizar uma queixa junto das Nações Unidas contra a Índia por eco-terrorismo, na sequência de ataques aéreos que danificaram uma reserva florestal. À altura, Malik Aslam, ministro para as alterações climáticas, precisou de sublinhar que não se tratava de uma piada, desde logo porque várias pessoas haviam ficado feridas. O terrorismo ambiental, ou ecológico, ainda é um conceito ambíguo e pouco autónomo, sobretudo no âmbito jus-internacional. Há autores que o definem como as acções realizadas por ambientalistas contra quem ameaça o ambiente e outros consideram eco-terroristas quem atenta contra o meio natural. Estes breves contributos apresentam o tema de forma não exaustiva, reflectindo sobre o seu enquadramento

Abstract: In March 2019, Pakistan announced its intention to formalize a complaint to the United Nations against India for eco-terrorism, following air strikes that damaged a forest reserve. At the time, Malik Aslam, the minister for climate change, had to emphasize that this was not a joke, especially as several people had been injured. Environmental or ecological terrorism is still an ambiguous and not very autonomous concept, especially in the international legal sphere. Some authors define it as actions carried out by environmentalists against those who threaten the environment, while others consider those who attack the natural environment to be eco-terrorists. These brief contributions present the topic in a non-exhaustive way, reflecting on its legal framework in the

* O presente texto resulta da revisão de uma comunicação com o mesmo título, que teve lugar na Faculdade de Direito da Universidade de Lisboa, a 6 e 7 de Junho de 2019, no âmbito do IX Encontro Luso-Espanhol de Professores de Direito Internacional e Relações Internacionais. Não obstante, por razões de tempo, a maioria das referências e citações mantiveram-se como no trabalho original, não tendo sido possível encetar uma investigação exaustiva do tema à altura da publicação.

jurídico na luta global contra o terrorismo. A investigação analisa os conceitos, sugerindo uma diferenciação funcional, e faz um levantamento dos diplomas internacionais relevantes, dando a conhecer um tema algo lateralizado.

Palavras-chave: Ambiente; Direito Internacional; Eco-terrorismo; Nações Unidas; Terrorismo.

global fight against terrorism. The research analyses the concepts, suggesting a functional differentiation, and makes a survey of the relevant international diplomas, shedding light on a somewhat lateralized theme.

Keywords: eco-terrorism; environment; International Law; United Nations; terrorism.

Sumário: 1. Introdução; 2. Terrorismo(s) ecológico(s); 2.1 Conceito comum; 2.2 Outra definição possível; 3. Regime jurídico-internacional dos atentados terroristas contra o meio ambiente; 3.1 Registos de eco-terrorismo; 3.2 A legislação internacional actual; 4. (In)suficiente protecção legal; 5. Conclusão.

“It’s only when something is gone, that we realise how much we miss it. Our capital city’s iconic ‘Iamsterdam’ sign, set in front of the Rijksmuseum, drew the admiration and camera lenses of millions of people worldwide. By bringing it back in altered state as ‘Iamazonia’, Greenpeace not only calls for the urgent protection of the largest remaining rainforest in the world, but also sends a strong message of solidarity to the Indigenous People and traditional communities who are protecting the Amazon against deforestation”^{***}

1. Introdução

Em Março de 2019, foi noticiado que o Paquistão iria apresentar uma queixa junto das Nações Unidas contra a Índia. Não houve desenvolvimentos relevantes até ao momento da escrita deste texto, mas o incidente não perdeu relevância. Tal surgiu no seguimento de ataques aéreos que danificaram

^{***} SIGRID DETERS, *Greenpeace turns world-famous ‘Iamsterdam’ landmark into solidarity message to save the Amazon*, 26 de Junho de 2019 (acesso em 15 de Maio de 2019).

pinheiros de uma reserva florestal perto de Balakot, no norte do país, a cerca de 40 quilómetros da fronteira. A Índia alegou ter destruído um campo de treino e morto centenas de terroristas, enquanto que o Paquistão negou a existência desse tipo de instalações. Alguns habitantes locais referiram que apenas um aldeão ficou ferido. O ministro paquistanês para as mudanças climáticas, Malik Aslam, disse que levaria o caso a instâncias internacionais, tendo considerado tratar-se de uma situação de terrorismo ambiental que teria provocado sérios danos materiais¹.

O ministro sentiu necessidade de acrescentar que a queixa não era uma piada, o que parece decorrer da reacção de estranheza com que o assunto terá sido recebido por parte do seu governo e de outros interlocutores. Apesar da actualidade tanto das questões de terrorismo como do impacto das actividades humanas no meio ambiente², a conjugação destes dois temas é um assunto algo lateral³, mormente pela doutrina que se debruça sobre Direito Internacional⁴. Mesmo alguns autores que têm vindo a estudar o

¹ Entre outros, ASIF SHAHZAD, *Pakistan to lodge U.N. complaint against India for 'eco-terrorism' forest bombing*, 28 de Fevereiro de 2019 (acesso em 10 de Maio de 2019); e MICHAEL BARBER, *Pakistan to lodge UN complaint against India for 'eco-terrorism'*, 1 de Março de 2019 (acesso em 10 de Maio de 2019).

² Vejam-se, por exemplo, genericamente, OLIVIER BARSALOU e MICHAEL HENNESSY PICARD, «International environmental law in an era of globalized waste», *Chinese Journal of International Law*, vol. 17, 2018, pp. 887-906; GEETANJALI GANGULY, JOANA SETZER e VEERLE HEYVAERT, «If at first you don't succeed: Suing corporations for climate change», *Oxford Journal of Legal Studies*, vol. 38, nº 4, 2018, pp. 841-868; ou JAAP SPIER, «The principles on climate obligations of enterprises: An attempt to give teeth to the universally adopted view that we must keep global warming below an increase of two degrees Celsius», *Uniform Law Review*, vol. 23, 2018, pp. 319-335. Apesar de não se debruçarem directamente sobre terrorismo ambiental, estes autores discutem alguns dos problemas actuais mais relevantes no que concerne ao desenvolvimento sustentável e alterações climáticas através de uma perspectiva multidisciplinar, mormente jurídica, sociológica e científica.

³ Como desenvolvem SIVAN HIRSCH-HOEFLER e CAS MUDDÉ, «“Ecoterrorism”: Terrorist threat or political ploy?», *Studies in Conflict & Terrorism*, vol. 37, nº 7, 2014 (pp. 586-603), p. 589, mesmo com os primeiros estudos sociais a serem documentados em 1996, “ecoterrorism has remained a relative fringe topic in terrorism studies, hardly meriting more than a tiny section in [encyclopedias] and textbooks, and rarely being the main focus of articles or books”.

⁴ SUE-MING YANG e I-CHIN JEN, «An evaluation of displacement and diffusion effects on eco-terrorist activities after police interventions», *Journal of Quantitative Criminology*, vol. 34, 2018 (pp. 1103-1123), p. 1104. Vejam-se as referências que estes autores fazem à pouca doutrina que conseguiram identificar a tratar de eco-terrorismo, nomeadamente DOUGLAS

terrorismo ambiental à escala global não o tendem a fazer da perspectiva adoptada neste artigo, como se verá adiante, ou tendem a vê-lo como algo a ser combatido internamente⁵. Esta é a premissa deste texto, cujo valor

LONG, *Ecoterrorism*, Nova Iorque, 2004; STEVE VANDERHEIDEN, «Eco-terrorism or justified resistance? Radical environmentalism and the “war on terror”», *Politics & Society*, vol. 33, nº 3, 2005, pp. 425-447; PAUL JOOSSE, «Leaderless resistance and ideological inclusion: The case of the Earth Liberation Front», *Terrorism and Political Violence*, vol. 19, nº 3, 2007, pp. 351-368, e o também seu «Elves, environmentalism, and “eco-terror”: Leaderless resistance and media coverage of the Earth Liberation Front», *Crime Media Culture*, volume 8, nº 1, 2012, pp. 75-93; REBECCA SMITH, «“Ecoterrorism”? A critical analysis of the vilification of radical environmental activists as terrorists», *Environmental Law*, vol. 38, 2008, pp. 537-576; JOSHUA FREILICH, STEVEN CHERMAK e JOSEPH SIMONE, «Surveying American state police agencies about terrorism threats, terrorism sources, and terrorism definitions», *Terrorism and Political Violence*, vol. 21, nº 3, 2009, pp. 450-475; JENNIFER CARSON, GARY LAFREE e LAURA DUGAN, «Terrorist and non-terrorist criminal attacks by radical environmental and animal rights groups in the United States, 1970-2007», *Terrorism and Political Violence*, vol. 24, nº 2, 2012, pp. 295-319; JENNIFER CARSON, «Counterterrorism and radical eco-groups: A context for exploring the series hazard model», *Journal of Quantitative Criminology*, vol. 30, 2014, pp. 485-504; e JENNIFER CARSON e BRAD BARTHOLOMEW, «Terrorism outside the proverbial vacuum: Implications for the moral context», *Deviant Behavior*, vol. 37, nº 5, 2016, pp. 557-572. Outros autores que se poderiam igualmente mencionar (na pesquisa feita em 2019) são LORENZ LUTHERER e MARGARET SIMON, *Targeted: The anatomy of an animal rights attack*, Oklahoma, 1993; DAVE FOREMAN e BILL HAYWOOD, *Ecodefense: A field guide to monkeywrenching*, 3.^a ed., Atenas, 2002; RANDALL AMSTER, «Perspectives on ecoterrorism: Catalysts, conflation, and casualties», *Contemporary Justice Review*, vol. 9, nº 3, 2006, pp. 287-301; DONALD LIDDICK, *Eco-Terrorism: Radical environmental and animal liberation movements*, Londres, 2006; MICHAEL LOADENTHAL, «Deconstructing “eco-terrorism”: Rhetoric, framing and statecraft as seen through the insight approach», *Critical Studies on Terrorism*, vol. 6, nº 1, 2013, pp. 92-117, e o também seu «Eco-terrorism? Countering dominant narratives of securitisation: A critical, quantitative history of the Earth Liberation Front (1996-2009)», *Perspectives on Terrorism*, vol. 8, nº 3, 2014, pp. 16-50; JEFF GRUENEWALD, KAYLA ALLISON-GRUENEWALD e BRENT KLEIN, «Assessing the attractiveness and vulnerability of eco-terrorism targets: A situational crime prevention approach», *Studies in Conflict & Terrorism*, vol. 38, nº 6, 2015, pp. 433-455; ou RIK SCARCE, *Eco-warriors: Understanding the radical environmental movement*, edição actualizada, Nova Iorque, 2016. Não obstante, toda a literatura aqui referida adopta uma óptica nacional de eco-terrorismo e define-o nos termos da primeira tipologia que será abordada, argumentando sobretudo com casos do Reino Unido e dos Estados Unidos da América. A vertente de terrorismo ambiental principalmente tratada neste texto tem sido, em geral, ignorada pela doutrina e pelos decisores políticos.

⁵ Veja-se, por exemplo, GERRY NAGTZAAM, *From environmental action to ecoterrorism?: Towards a process theory of environmental and animal rights oriented political violence*, Cheltenham, 2017.

acrescentado prende-se com a exploração, embora breve e não exaustiva ou sequer amplamente doutrinária, de uma vertente do conceito de eco-terrorismo e da sua protecção jurídico-internacional menos comum na literatura e mesmo nos estudos de segurança.

Na primeira secção, serão analisados os dois principais tipos de terrorismo ambiental e será explicado o objecto específico de análise deste trabalho. A seguinte secção dará conta de exemplos de eco-terrorismo e tentará apurar quais os instrumentos jurídicos internacionais actualmente em vigor que tutelam as acções terroristas contra o ambiente e que regulam, de certo modo, o combate a este fenómeno. Por fim, na última secção tecem-se comentários sobre o regime, apresentando-se algumas propostas de futuro – um futuro visto desde 2019, já que não foi possível uma completa actualização deste texto no momento da sua revisão e publicação.

2. Terrorismo(s) ecológico(s)

2.1. Considerações gerais

Esta primeira secção pretende explorar os subtipos de terrorismo ambiental e individuar o objecto de interesse do estudo. Apesar de o conceito de terrorismo ser muito utilizado a nível internacional em estudos políticos, sociais e jurídicos⁶, não deixa de ser difícil de concretizar uma definição⁷. Terrorismo é um dos conceitos mais polissémicos de Direito Internacional

⁶ ANNA ALEKSEEVA, ALEKSEY ANISIMOV e ANATOLIY RYZHENKOV, «Environmental terrorism, environmental radicalism and measures to counteract them», *Environmental Policy and Law*, vol. 47, nº 1, 2017 (pp. 24-34), p. 24.

⁷ DANIEL SCHWARTZ, «Environmental terrorism: Analyzing the concept», *Journal of Peace Research*, vol. 35, nº 4, 1998 (pp. 483-496), p. 485. CARSON e BARTHOLOMEW, «Terrorism outside the proverbial vacuum», cit., p. 557, usam a definição reproduzida por GARY LAFREE e LAURA DUGAN, «Introducing the global terrorism database», *Terrorism and Political Violence*, vol. 19, 2007 (pp. 181-204), p. 184, a partir dos *Pinkerton Global Intelligence Services*. Terrorismo, para estes autores e também no âmbito deste artigo, consiste no uso ou ameaça do uso da força e violência ilegais para atingir objectivos políticos, económicos, religiosos ou sociais através do medo, coerção ou intimidação. No entanto, CARSON e BARTHOLOMEW admitem que este é um tema relativamente novo no campo da criminologia, tendo vindo a ser desenvolvido de forma mais acentuada, pelo menos com dados empíricos, a partir dos ataques terroristas de 2001 que ocorreram nos Estados Unidos da América.

e está em permanente actualização. Já há considerável literatura a tratar dos seus diversos significados, sendo que importa apenas aqui questionar, como faz Shannon O’Lear, se caberá nesta noção uma componente ambiental⁸ e se não haverá o risco de se tornar uma expressão «*overused and under thought*»⁹.

Também não são unívocos os diversos tipos de terrorismo, muito embora uns estejam mais consolidados na literatura e na opinião pública do que outros. Terrorismo nuclear, por exemplo, é melhor conhecido do que terrorismo tecnológico. Seja como for, não será aqui desenvolvida uma definição específica de terrorismo nem se entrará nas querelas doutrinárias relativamente a esta noção. Este artigo adopta antes alguns dos traços mais usados pelos autores para se referirem a este fenómeno no sentido de criar uma base de trabalho ontológica útil e inteligível, considerando o terrorismo como o uso ou ameaça do uso ilegítimo da força ou violência para intimidar ou coagir forças políticas ou populações civis em favor de certos interesses, mormente de natureza política, social, económica, religiosa, através do medo e da coerção¹⁰.

2.2. Conceito comum

Terrorismo ambiental, também designado por terrorismo ecológico ou eco-terrorismo¹¹, é um conceito amplo, sendo entendido sobretudo de

⁸ SHANNON O’LEAR, «Environmental terrorism: A critique», *Geopolitics*, vol. 8, nº 3, 2003 (pp. 127-150), p. 131.

⁹ *Id.*, p. 146.

¹⁰ Esta é, em certa medida, a visão acolhida pelo *Federal Bureau of Investigation* norte-americano e por autores como ELIZABETH CHALECKI, «A new vigilance: Identifying and reducing the risks of environmental terrorism», *Global Environmental Politics*, vol. 2, nº 1, 2002 (pp. 46-64), p. 47. No entanto, esta autora, entre outros aspectos limitativos, acaba por restringir o terrorismo ambiental aos ataques a recursos naturais, assim deixando de lado ataques aos espaços abióticos que não representem necessariamente um benefício económico óbvio e directo para as populações humanas, como reservas ou parques naturais protegidos. Esta posição estrita não é seguida aqui.

¹¹ Autores como CHALECKI, «A new vigilance», cit., pp. 48 ss.; JOSÉ MESTRE, «Segurança ambiental e terrorismo», *Revista Militar*, nº 2248, 2006 (pp. 1-27), p. 16; ou VALERIA VILLA, *et al.*, «Development of an economic model for the allocation of preventive security measures against environmental and ecological terrorism in chemical facilities», *Process*

duas maneiras distintas tanto pela doutrina jurídica como noutras áreas de estudo. A primeira vê este tipo de criminalidade como acções ilegais levadas a cabo por agentes não estatais para promover mudanças nos comportamentos, mormente do sector empresarial e das forças políticas, em relação ao meio ambiente. Como escreveu Martin Heger, este tipo de terrorismo pode ser sintetizado como «*ecologically motivated terrorism*»¹², seguindo na esteira de algumas teorias como o bio-centrismo ou a ecologia profunda¹³.

Esta definição é resultado do que grupos ambientalistas mais extremados denominam por acção directa em prol da preservação do ambiente e está em linha com a divulgação das suas mensagens ideológicas¹⁴. Apesar de a maioria destas acções serem pacíficas, tomando a forma de greves ou demonstrações, podem suceder escaladas de violência que resultam na prática de crimes ou mesmo actos terroristas. Como alude José Mestre, porém, nem sempre são claros os discursos políticos nos meios de comunicação

Safety and Environmental Protection, vol. 109, 2017 (pp. 311-339), p. 312, *inter alia*, segue SCHWARTZ, *Environmental terrorism*, cit., p. 484, ao distinguir eco-terrorismo de terrorismo ambiental ou «*enviro-terrorism*», considerando que aquele se refere a actos radicais ilegais cometidos em prol do ambiente, tanto através de danos à propriedade ou à vida e integridade de pessoas como por meio de activismo não violento, levados a cabo quer por indivíduos quer por grupos em protesto contra o que entendem ser a destruição ou depleção do ambiente. Já o terrorismo ambiental, por outro lado, é tido como a criação ilegítima de danos severos ao meio ambiente por pessoas ou organizações através da perturbação dos recursos e propriedades ambientais. Esta é uma classificação que se assemelha às duas vertentes de terrorismo ecológico identificadas neste artigo, muito embora não se faça esta distinção terminológica porque não parece haver suficiente distância óptica e hermenêutica entre os termos «terrorismo ambiental», «terrorismo ecológico» e «eco-terrorismo» para que se possam usar estas expressões para aludir a diferentes referentes epistemológicos. Assim sendo, estas três noções serão usadas como sinónimos com as duas variantes conceptuais delineadas neste trabalho. Elas correspondem, na verdade, a uma mesma natureza e criar distinções rígidas entre termos tão semelhantes só aprofunda uma complexificação desnecessária e pouco útil da realidade a tratar e classificar pelo Direito.

¹² MARTIN HEGER, «Terrorist attacks against the natural environment: A phantom or a real danger», *German Law Journal*, vol. 13, nº 9, 2012 (pp. 1066-1074), p. 1066.

¹³ Para mais desenvolvimentos, veja-se GERRY NAGTZAAM e PETE LENTINI, «Vigilantes on the high seas?: The Sea Shepherds and political violence», *Terrorism and Political Violence*, vol. 20, nº 1, 2008 (pp. 110-133), pp. 112 ss..

¹⁴ YANG e JEN, «An evaluation of displacement», cit., p. 1104.

social que se referem a estas práticas¹⁵, sendo que tende a verificar-se algum empolamento mediático dos seus efeitos, para que, como escreve Steve Cooke, se possam categorizá-las como terrorismo¹⁶ e, de alguma forma, se descredibilizem os seus autores. O elemento comum tende a ser a comissão de danos económicos de forma dolosa, sendo raros, em qualquer situação, os danos causados a seres humanos. Os casos mais paradigmáticos destes crimes consistem em vandalismo, sabotagem (ou eco-tagem, na acertada expressão de Steve Vanderheiden¹⁷), detonação de engenhos explosivos e fogo posto em instalações industriais que, no entender daqueles grupos ambientalistas, utilizam animais ou que exploram o meio ambiente de forma abusiva, mormente empresas de cosmética, exploração madeireira, pesca e caça de baleias ou criação intensiva de gado.

Este tipo de terrorismo tem sido estudado sobretudo a nível nacional¹⁸, sendo um fenómeno conhecido nos Estados Unidos da América desde os anos 70 do século passado. Devido ao seu crescente impacto social e económico, no início da década de 90, o governo federal iniciou uma campanha de combate ao terrorismo ecológico interno, tendo ficado conhecidos os nomes dos grupos ambientalistas *Earth First!*, *Earth Liberation Front* e *Animal Liberation Front*¹⁹. É neste contexto que nasce a expressão eco-terrorismo, sendo que Josh Leamons considera que tenha sido utilizada pela primeira vez em 1983²⁰. Neste período de crescente sublevação social em prol do am-

¹⁵ MESTRE, «Segurança ambiental e terrorismo», cit., p. 16.

¹⁶ STEVE COOKE, «Animal rights and environmental terrorism», *Journal of Terrorism Research*, vol. 4, nº 2, 2013 (pp. 26-35), pp. 26-27.

¹⁷ STEVE VANDERHEIDEN, «Radical environmentalism in an age of antiterrorism», *Environmental Politics*, vol. 17, nº 2, 2008 (pp. 299-318), pp. 300 ss..

¹⁸ Não obstante, há já um acervo relevante de estudos sobre eco-terrorismo a nível internacional que adoptam esta primeira tipologia, nomeadamente no que respeita a activismo em alto mar. Veja-se STEFANO DOMINELLI, «Evolutionary trends in maritime piracy: A possible assessment of eco-activists' conduct», *Australian International Law Journal*, vol. 21, 2014 (pp. 41-54), p. 43, bem como as várias referências doutrinárias aí feitas, e, em geral, ALANA PRESTON, «Eco-terrorism in the southern ocean: A dangerous byproduct of the tangled web of international whaling conventions and treaties», *Whittier Law Review*, vol. 34, nº 1, 2012, pp. 117-139.

¹⁹ MICHAEL LOADENTHAL, «Activism, terrorism, and social movements: The “green scare” as monarchical power», em *Narratives of identity in social movements, conflicts and change*, Landon Hancock (ed.), Bingley, 2016 (pp. 189-226), pp. 189-190.

biente, algumas empresas privadas começaram a apelidar os ambientalistas de eco-terroristas para os estigmatizar²¹ junto da opinião pública e do governo. O eco-terrorismo chegou mesmo a ser listado como a mais grave ameaça terrorista doméstica pelo *Federal Bureau of Investigation* em 2005²².

2.3. Outra definição possível

A segunda definição de eco-terrorismo é sobretudo uma construção doutrinária, sendo menos conhecida e estudada²³, muito embora tenha

²⁰ JOSH LEAMONS, «Eco-terrorism: A legal update on the laws protecting scientific research from extremist activists», *Journal of Biosecurity, Biosafety and Biodefense Law*, vol. 6, nº 1, 2015 (pp. 23-42), p. 25, baseado no trabalho de SMITH, «“Ecoterrorism”?», cit., p. 546. DAVID SUMNER e LISA WEIDMAN, «Eco-terrorism or eco-tage: An argument for the proper frame», *Interdisciplinary Studies in Literature and Environment*, vol. 20, nº 4, 2013 (pp. 855-876), p. 857, escrevem que foi cunhada por Ron Arnold num artigo da publicação mensal da Fundação *Reason*.

²¹ YANG e JEN, «An evaluation of displacement», cit., p. 1104. Para um estudo mais aturado das origens do fenómeno nos Estados Unidos da América, veja-se SEAN EAGAN, «From spikes to bombs: The rise of eco-terrorism», *Studies in Conflict and Terrorism*, vol. 19, nº 1, 1996, pp. 1-18.

²² ROBERT MUELLER, *Testimony*, 5 de Abril de 2005 (acesso em 24 Maio de 2019). No testemunho do director do *Federal Bureau* da altura pode ler-se que os extremistas em prol do ambiente e dos direitos animais estão colocados no topo da lista de ameaças terroristas internas. A violência à altura justificava a categorização de algumas práticas como de natureza terrorista, sendo que se estima que os movimentos radicais em prol do ambiente terão provocado, entre 1970 e 2007, prejuízos materiais nos Estados Unidos da América de cerca de 200 milhões de dólares. No comunicado pode ler-se, em concreto, que «[s]erious incidents of animal rights/eco-terrorism decreased in 2004 (...). Following a rash of serious incidents of animal rights/eco-terrorism, including a \$50 million arson in San Diego and two bombing incidents in the San Francisco area, law enforcement authorities achieved several significant successes which have likely deterred additional terrorist activity. Despite these successes, we anticipate that animal rights extremism and eco-terrorism will continue to threaten certain segments of government and private industry, specifically in the areas of animal research and residential/commercial development».

²³ Muitas vezes vista de maneira limitada e, portanto, incompleta. Aliás, esta segunda visão de terrorismo ambiental é encarada e descrita por certos autores de tal forma que acabam por rejeitá-la sem a realmente estudarem na sua potencialidade. Veja-se o caso de O'LEAR, «Environmental terrorism», cit., p. 147, que considera erradamente que «[t]he term ‘environmental terrorism’ would seem to suggest that phenomena under discussion are peacetime events not initiated by states [and that, therefore,] this interpretation misses important

começado a ser divulgada já no final da década de 90²⁴. Terrorismo ambiental pode igualmente designar os actos ilegais levados a cabo por agentes terroristas que provocam, normalmente com violência, danos graves no ambiente, com o objetivo de coagir forças políticas ou populações civis através do medo e em prol de certos interesses. A protecção do meio ambiente tende a ser o ou um dos principais objectivos no primeiro tipo de terrorismo ecológico, enquanto que aqui o meio ambiente é o mais relevante ou um dos mais relevantes alvos deste tipo de crimes.

Convém precisar alguns dos componentes desta definição abrangente. Na esteira de Daniel Schwartz, o dano ao ambiente não pode ser meramente incidental²⁵ (*i.e.*, não necessário) nem deve ser irrelevante. Ademais, como explicam Anna Alekseeva, Aleksey Anisimov e Anatoliy Ryzhenkov, não é forçoso que se usem meios químicos, nucleares ou bacteriológicos para se estar perante terrorismo ambiental²⁶. O que releva é o binómio de intenção criminosa, o elemento volitivo, e dano significativo provocado ao ambiente. Nem também importa, ou deve importar, que o dano seja cometido num ambiente misto (humano e natural) ou inteiramente natural²⁷. Para estes autores, a principal característica da segunda vertente deste tipo de terrorismo é, precisamente, a intimidação de populações ou agentes governativos através da ameaça de danos consideráveis ao meio ambiente, normalmente com consequências a nível humano²⁸. De facto, é possível haver actos com impacto semelhante no ambiente sem qualquer intenção de se intimidar ou promover alguma mudança de atitudes sócio-políticas. No entanto, não estaremos aí perante casos de terrorismo. Dependendo da gravidade dos danos causados, poderá ocorrer, por exemplo, um ecocídio, ou seja, a

scales and types of hostile, unexpected activity that might be eclipsed by an unnecessarily narrow approach». Não obstante, esta construção é sugerida pelo próprio autor e não tem nenhuma base jurídica ou factual que a sustente.

²⁴ De forma paradigmática, SCHWARTZ, «Environmental terrorism», cit., p. 484.

²⁵ *Id.*

²⁶ ALEKSEEVA, ANISIMOV e RYZHENKOV, «Environmental terrorism», cit., p. 26.

²⁷ Apesar de os seres humanos fazerem parte do meio ambiente, a distinção aqui é sociológica e não estritamente biológica. Serve para se compreender, de forma clara, que em causa na expressão ambiente natural estão os animais não humanos e os demais elementos do meio natural biótico e até abiótico.

²⁸ ALEKSEEVA, ANISIMOV e RYZHENKOV, «Environmental terrorism», cit., p. 25.

destruição massiva de flora ou fauna, a contaminação da atmosfera e recursos hídricos ou a comissão de acções que levem a uma catástrofe ecológica. O elemento da vontade é, em bom rigor, tão essencial como o elemento do dano para se estar perante um acto de terrorismo²⁹ e para o distinguir de outros tipos objectivos de crime, bem como de simples incidentes ou de más práticas ambientais.

Importa realçar que, ao contrário da primeira vertente de eco-terrorismo, esta pode reportar-se a um crime de natureza verdadeiramente jus-internacional. Mesmo que ainda não haja uma tipificação clara em legislação transnacional, como se verá adiante, estão reunidos os critérios materiais para que se considere estarmos perante uma realidade juridicamente relevante e sindicável pelo Direito Internacional. Seguindo a categorização de Ben Saul³⁰, em primeiro lugar, estará em causa uma conduta grave de interesse internacional – neste caso, a provocação de danos ao meio biótico e abiótico e, quiçá, aos próprios seres humanos. Em seguida, verifica-se o elemento transnacional: mesmo que se contenham, em casos concretos, ao território de um só país, os actos de terrorismo tendem a afectar interesses, bens e valores que ultrapassam as fronteiras geopolíticas e merecem, assim, protecção internacional. No caso do eco-terrorismo, não só a qualidade e preservação ambientais são interesses difusos a tutelar pela comunidade internacional independentemente de práticas nocivas como muitos dos efeitos do terrorismo ambiental poder-se-ão sentir para lá de quaisquer extremas, como sucede com quase todos os problemas ambientais globais³¹. Se a ameaça à paz e segurança regionais tende a ser um efeito intrínseco do terrorismo em geral, no caso do terrorismo ecológico somam-se as ameaças à qualidade do meio ambiente e vida de populações humanas, animais e vegetais. Finalmente, o terrorismo ambiental afecta a comunidade internacional, o conjunto de participantes do sistema global, e é-lhe transversal. Independentemente da visão que se

²⁹ Não será aqui abordada a questão das omissões, especialmente por serem de difícil enquadramento numa lógica de actividade terrorista. Seja como for, é possível que se consigam conjugar e convém não afastar à partida a prática de actos terroristas contra o meio ambiente por omissão. Também não será aprofundado o ecocídio como categoria próxima de crime, muito embora seja um assunto premente na agenda legislativa europeia e internacional da actualidade.

³⁰ BEN SAUL, *Defining terrorism in international law*, Oxford, 2008, pp. 11 ss..

³¹ MESTRE, «Segurança ambiental e terrorismo», cit., p. 12..

adopte desta comunidade – seja uma posição mais clássica e monolítica assente na figura do Estado-nação ou uma mais dinâmica e multipolarizada –, o meio ambiente é um bem comum e o terrorismo um perigo horizontal que une, ou deveria unir, na expressão de Jürgen Habermas, «the world into an involuntary community of shared risks»³².

Apesar de alguns grupos ambientalistas considerarem que eco-terroristas são, desde logo, quem explora de forma não sustentável o planeta, a atmosfera e os recursos naturais em nome do progresso e do capitalismo, esta não é a perspectiva que mais releva para este artigo. Noutra plano, é mister referir que um conceito próximo de eco-terrorismo é o de terrorismo biológico³³. É possível usá-los como sinónimos mas alguns autores preferem limitar o escopo do bio-terrorismo ao uso de agentes patogénicos, toxinas ou outros elementos químicos prejudiciais à saúde contra populações humanas para coagir ou intimidar governos e indivíduos, desviando-se assim da provocação de danos ao ambiente natural³⁴. O elemento instrumental parece aqui ser preponderante, ou seja, o conjunto de meios usados para alcançar os objectivos da agenda ideológica. Esta é igualmente a posição adoptada no presente texto, o que permite imprimir alguma precisão aos termos usados. O terrorismo biológico só estará incluído neste tipo de eco-terrorismo se tiver um impacto relevante no meio ambiente, como sugerem Claudiu Sbârcea, Lucian Lerescu e Mariana Jinga na sua definição do conceito³⁵.

O ataque com gás *sarin* que teve lugar em Tóquio a 20 de Março de 1995³⁶, por exemplo, não teve como alvo o ambiente natural nem nele

³² JÜRGEN HABERMAS, *The inclusion of the other: Studies in political theory*, Cambridge, 2005, p. 186.

³³ Para um estudo mais aprofundado do bio-terrorismo do ponto de vista das ciências naturais, veja-se MAHDI BALALI-MOOD, MOHAMMAD MOSHIRI e LEILA ETEMAD, «Medical aspects of bio-terrorism», *Toxicon*, vol. 69, 2013, pp. 131-142.

³⁴ BARRY KELLMAN, «Biological terrorism: Legal measures for preventing catastrophe», *Harvard Journal of Law and Public Policy*, vol. 24, nº 2, 2001 (pp. 425-488), p. 426.

³⁵ CLAUDIU SBÂRCEA, LUCIAN LERESCU e MARIANA JINGA, «Bio-terrorism: Still interesting or concerning nowadays?», *Romanian Journal of Military Medicine*, vol. 117, nºs 3-4, 2014, pp. 5-10, incluem na noção de bio-terrorismo não só a provocação de danos à integridade física e vida de seres humanos mas também de animais e plantas. Deste modo, o terrorismo biológico poderá ser tomado como uma variante ou especificação de eco-terrorismo.

³⁶ BBC, *Tokyo Sarin attack: Japan executes last Aum Shinrikyo members on death row*, 26 de Julho de 2018 (acesso em 27 de Maio de 2019). Para mais detalhes sobre a organização

provocou efeitos graves ou duradouros, tendo-se restringido a afectar populações humanas³⁷. Tendo sido classificado como ataque terrorista, o tipo de dano leva a qualificar esta situação como terrorismo biológico mas não ecológico³⁸. Já o ataque à estação hidroeléctrica de *Baksan*, na região russa de *Kabardino-Balkaria*, a 21 de Julho de 2010, pode ser considerado como uma tentativa de terrorismo ambiental. Alguns indivíduos mascarados entraram nas instalações da estação de madrugada, matando duas pessoas e fazendo explodir dispositivos artesanais que destruíram dois geradores e causaram um incêndio na sala de controlo. Apesar de o impacto no meio ambiente pretendido ter sido evitado, o objectivo era perturbar o fornecimento

responsável por este ataque, veja-se IAN READER, *Religious violence in contemporary Japan: The case of Aum Shinrikyo*, Richmond, 2000.

³⁷ Em sentido oposto, HEGER, «Terrorist attacks against the natural environment», cit., p. 1067, considera que, para ser um caso de eco-terrorismo, basta a utilização abusiva de um recurso natural como arma contra populações humanas. Nesta situação em concreto, como o gás *sarin* foi libertado no ar e tornou-o tóxico para os seres humanos, o autor considera que é um caso de terrorismo ambiental. No entanto, esta visão antropocêntrica e especista não parece permitir uma verdadeira independência entre o terrorismo ecológico e a provocação de danos ou ameaça desses danos em seres humanos – independência essa que é um ponto essencial para uma visão mais abrangente da realidade, uma melhor protecção jurídica do meio natural e uma valorização adequada do ambiente como bem jurídico autónomo a tutelar. Ou seja, a ameaça ou efectiva provocação de danos em seres humanos não deve ser um requisito necessário para se estar perante eco-terrorismo, como se pretende demonstrar neste artigo, pois que o ambiente deve ser considerado, se já não o é, como um bem jurídico próprio e que releva proteger *per se*. Mesmo que nenhum ser humano possa ser afectado na sua saúde, integridade ou vida por um atentado terrorista, a provocação de danos relevantes ao ambiente no quadro de uma actividade terrorista e com a intenção de coagir populações civis ou governos de forma ilegal deve ser, de forma inequívoca, considerada como terrorismo ecológico. No caso em concreto, por exemplo, o ar respirável ficou contaminado com o gás *sarin* mas este, ao fim de algum tempo, dissipou-se e não provocou danos concretos ao ar. Donde, não está verificado o elemento do dano grave ao ambiente e, por isso, não deve ser considerado como eco-terrorismo, nesta vertente.

³⁸ Enquanto que a expressão terrorismo ambiental está sobretudo associada nos Estados Unidos da América, como se viu, a terrorismo interno de grupos ambientalistas que causam danos para alertar para a protecção do ambiente, na Rússia, pelo contrário, ALEKSEEVA, ANISIMOV e RYZHENKOV, «Environmental terrorism», cit., p. 24, referem que a doutrina que trata de terrorismo ambiental normalmente associa-o ao segundo tipo de terrorismo, muito embora só o considere relevante quando cause danos em seres humanos. Assim sendo, também boa parte dos autores russos não consideram o tipo de terrorismo que aqui se analisa em detalhe.

eléctrico e destruir a estação, o que levaria a danos ambientais de relevo³⁹. Atenção que o dano humano, tal como qualquer dano material que não afecte o ambiente natural, pode existir numa situação de terrorismo ambiental e não afasta esta tipologia. No entanto, o dano ambiental tem de ser querido ou necessário à prática do crime, tem de existir⁴⁰ e tem de ser relevante, sob pena de se estar perante outra classificação de terrorismo ou, inclusivamente, outro tipo de crime.

Convém clarificar que os danos humanos são tendencialmente um elemento comum na definição de terrorismo. Embora não seja consensual na literatura⁴¹, a morte ou ofensa à integridade física de pessoas não devem ser critérios obrigatórios para se considerar certas acções como actos eco-terroristas. O contrário levaria a afastar esta classificação em determinados cenários e, quiçá, tanto diminuir a relevância do ambiente como bem jurídico valioso como descurar o impacto psicológico que determinados ataques podem provocar junto das populações, mesmo que apenas o meio natural seja afectado.

É mister aqui atender ao valor jurídico da natureza como bem a proteger de forma independente e autónoma daqueles outros bens. A valorização que tem tido o ambiente em legislações penais nacionais em diversos países deve (poder) reflectir-se a nível internacional. Tal não diminui a certeza

³⁹ MAXIM TKACHENKO, *Power plant 'terror' attack kills 2 in Russia*, 21 de Juho de 2010 (acesso em 27 de Maio de 2019).

⁴⁰ Ou estar no *iter* criminoso, mesmo que seja evitado ou prevenido de alguma forma.

⁴¹ Por exemplo, HEGER, «Terrorist attacks against the natural environment», cit., p. 1070, considera que «[i]n order to label a crime as terrorist it is required that the pollution or destruction of the natural environment is combined with the intent to kill or to harm people as part of a terrorist plan». E acrescenta que «it makes a difference whether someone just wants to destroy the natural environment or wants to destroy the natural environment combined with the intent to kill or to harm people». Tal parece ser desnecessário, porém, como critério para se verificar a comissão de terrorismo ambiental. Desde logo, a intenção de matar ou de ferir seres humanos é um critério diferente de haver um plano terrorista. O plano, parte da *mens rea*, pode passar por não causar este tipo de danos, directa ou mesmo indirectamente, e manter-se, mesmo assim, tanto a coacção como o próprio plano criminoso do tipo objectivo de crime de terrorismo – e que afecta, em particular, o ambiente. Que crime seria nesse caso? A classificação e os danos devem ser suficientes pelo valor do bem jurídico em causa; ou seja, a diferença deve residir antes na destruição do ambiente com um fim coactivo, não na causa (necessária ou aceite) de danos humanos.

jurídica e a firmeza do conceito de terrorismo por duas razões. Por um lado, o terrorismo ofende, ou pode ofender, outros bens e valores humanos, como a integridade psicológica, a liberdade ou a segurança. Qualquer prática de terrorismo ambiental, mesmo levada a cabo longe de centros urbanos, é passível de ter estas repercussões. Por outro lado, o elemento volitivo de exercício de influência ou pressão ilegítima através da coacção e do terror sob populações civis ou agentes governativos no seio de uma agenda criminosa terá sempre de ser verificado para que se esteja perante um caso de terrorismo, em geral, e terrorismo ambiental, em especial.

Como avançam Gerry Nagtzaam e Pete Lentini, a violência que está na base do terrorismo não tem de ser exercida contra seres humanos para que os terroristas obtenham as mudanças que pretendem por intermédio do medo⁴². E o elemento volitivo mantém o cariz humano na definição legal de terrorismo, sem ser necessário adoptar uma visão antropocêntrica limitativa que descarte o meio natural como bem jurídico que pode ser alvo de práticas criminosas de elevada gravidade e que devem ter sanções adequadas⁴³.

Um último ponto é devido para esclarecer de forma mais aturada o elemento da vontade, a intenção de provocar danos ambientais. Há crimes e actos de terrorismo que incidentalmente ou necessariamente causam danos ao ambiente. Enquanto que, no primeiro caso, não parece haver uma situação de terrorismo ambiental, muito embora se devam pesar os efeitos do ataque em concreto para apurar a classificação do tipo objectivo de crime de forma casuística, já quando o dano ao ambiente ocorre de forma necessária ou directa com a comissão destes crimes, como o uso de explosivos ou incêndios em florestas, é possível dizer, verificados os demais

⁴² NAGTZAAM e LENTINI, «Vigilantes on the high seas?», cit., p. 111.

⁴³ Atenção que a relevância do ambiente como bem jurídico a proteger de forma autónoma não significa que o meio ambiente é axiologicamente mais relevante do que a vida humana. SCHWARTZ, «Environmental terrorism», cit., p. 494, faz alusão precisamente a este *caveat* dizendo que categorizar um acto de terrorismo em que, por exemplo, haja perda de vidas humanas como eco-terrorismo não significa, por um lado, que a única 'vítima' relevante seja o ambiente e que, por outro, se devam elevar as preocupações ecológicas acima das preocupações com os seres humanos. Isto nem sequer é uma abertura do debate: a categorização aqui usada serve para que não se desconsidere o ambiente em casos de actos terroristas sem vítimas humanas e não o oposto.

requisitos do crime, que se está perante uma real situação de terrorismo ecológico. É claro que isto não afasta ou diminui outras categorizações ou a importância dos danos humanos, como visto. O terrorismo nuclear, por exemplo, é tendencialmente também eco-terrorismo e nada obsta em termos de classificação jurídico-hermenêutica a sua adjectivação cumulativa que descreve de forma mais completa a realidade. Pelo contrário, pois que assim se tutela (ou poderá tutelar) melhor os diversos interesses juridicamente atendíveis. Aliás, é relevante que todos os efeitos da violência exercida sejam ponderados na interpretação do crime: o impacto físico no meio ambiente não tende a estar confinado ao conjunto de efeitos directos e imediatos do acto criminoso concreto. Já Schwartz alertava, na viragem do século, para o facto de que a «interconnectedness of the environment» faz com que os efeitos da destruição ecológica possam ser mais vastos do que inicialmente possa parecer⁴⁴.

Alekseeva, Anisimov e Ryzhenkov sublinham a necessidade de se verificarem danos ambientais para a categorização do crime, aditando que parte da literatura russa classifica como eco-terrorismo a intimidação de populações através de ameaças à destruição de indústrias em zonas urbanas que podem provocar desastres ecológicos⁴⁵. Apesar de estas ameaças terem como alvo principal a saúde e vida humanas, ao surgirem danos significativos no meio ambiente, como derrames de produtos tóxicos, poluição atmosférica ou destruição da biodiversidade⁴⁶, para além dos danos materiais e humanos, devem ser classificadas como ameaças ecológicas no sentido aqui explorado. Isto porque, com a comissão destes actos, é certo que se verificarão danos ambientais graves, isto é, danos que irão decorrer directa ou necessariamente na sequência da prática daqueles actos e que devem ser previstos, ou deveriam constar, no espírito ou intenção criminosa, na *mens rea* dos agentes terroristas.

⁴⁴ SCHWARTZ, «Environmental terrorism», cit., p. 485.

⁴⁵ ALEKSEEVA, ANISIMOV e RYZHENKOV, «Environmental terrorism», cit., p. 25.

⁴⁶ Alguns exemplos concretos que os autores referem a partir de outros autores são a infecção de populações humanas indirectamente através da transmissão de agentes contagiosos administrados em aves e peixes, a queima de zonas de floresta e selva, a libertação de materiais radioactivos ou a destruição de estruturas e estações hidráulicas ou nucleares.

Fica claro que a literatura tem explorado o conceito de terrorismo, criando categorias de acordo com os meios que os agentes utilizam, os danos provocados, as causas em que se baseiam as reivindicações terroristas e até mesmo a dimensão territorial dos ataques. Também se pode falar de tipos de terrorismo consoante os seus efeitos, os alvos em questão, entre outros factores⁴⁷. O terrorismo ecológico tem, até desde antes dos eventos de 11 de Setembro de 2001, capacidade para se tornar um campo de investigação próprio e, segundo O’Lear, a sua taxinomia deveria ser incluída na definição mais ampla e assente de terrorismo⁴⁸.

A vertente em que o ambiente é um dos principais alvos desta criminalidade é, curiosamente, aquela que é menos conhecida. Será porque o fenómeno ainda é abordado sobretudo de um ponto de vista dos regimes jurídicos nacionais ou, quiçá, porque o ambiente é colocado em segundo plano nos principais fóruns sobre terrorismo? Ou porque a expressão terrorismo ambiental é usada, muitas vezes, de forma leviana e juridicamente incorrecta⁴⁹? Alekseeva, Anisimov e Ryzhenkov parecem responder, parcialmente, à segunda parte da primeira questão, ao dizerem que «[i]f an act of terrorism has an impact [upon] elements of the natural environment but does not affect the human environment, it is less likely to achieve [its] goals, as most people are motivated by self-interest and therefore primarily concerned about their own safety and wellbeing»⁵⁰.

⁴⁷ ALEKSEEVA, ANISIMOV e RYZHENKOV, «Environmental terrorism», cit., pp. 26 ss., incluem mesmo na noção de terrorismo ambiental diversos tipos de terrorismo nem sempre classificados como eco-terrorismo, nomeadamente tecnológico, nuclear, químico e biológico (que inclui terrorismo agrário, isto é, actos terroristas que levam, por exemplo, à morte de animais usados em actividades de agropecuária ou à contaminação de vegetação). Não obstante, não parece que esta classificação seja isenta de críticas ou que tenha valor acrescentado para se compreender o tipo de terrorismo ambiental aqui estudado.

⁴⁸ O’LEAR, «Environmental terrorism», cit., p. 127.

⁴⁹ Para um aprofundamento deste assunto, veja-se SCHWARTZ, «Environmental terrorism», cit., pp. 493-494, em particular quando refere o uso do conceito de forma retórica por agências e representantes políticos.

⁵⁰ ALEKSEEVA, ANISIMOV e RYZHENKOV, «Environmental terrorism», cit., p. 26.

3. Regime jurídico-internacional dos atentados terroristas contra o meio ambiente

3.1. Considerações gerais

Nesta secção analisa-se o regime jurídico de Direito Internacional que se debruça sobre o terrorismo ambiental, bem como os diplomas que espelham preocupações com a salvaguarda do ambiente em virtude de ataques terroristas. Na verdade, a menor atenção dada pela doutrina a este fenómeno e à exploração da sua definição é reflexo da falta de regulação jus-internacional, sendo que não há legislação global que se debruce de forma exclusiva e evidente sobre o terrorismo ecológico na vertente aqui tratada.

Não obstante, a verdade é que o desenvolvimento tecnológico e os fluxos mundiais de armas têm tornado cada vez mais fácil para organizações terroristas cometerem actos criminosos com um impacto relevante no ambiente natural, nomeadamente através do recurso a meios biológicos⁵¹. Apesar disso, a cooperação internacional de combate ao eco-terrorismo é insipiente, quiçá por alguma ignorância deste fenómeno ou mesmo por falta de vontade política (ou por se enquadrar de forma secundária na luta global contra o terrorismo). Para Alekseeva, Anisimov e Ryzhenkov é necessário criar-se um quadro jurídico e regulatório harmonizado a nível internacional⁵², sendo que uma possível explicação para que não haja (mais) interesse no terrorismo ambiental⁵³ poderá ser o reduzido número de ataques terroristas que tenham provocado danos graves ao meio ambiente. Assim sendo, antes de se analisar o regime jurídico, é preciso apurar se há uma base factual de incidentes terroristas que justifique uma maior atenção a este fenómeno, tanto na literatura como a nível institucional⁵⁴.

⁵¹ SCOTT CARY, «The tipping point: Biological terrorism», *Journal of Strategic Security*, vol. 2, nº 3, 2009 (pp. 13-24), p. 17.

⁵² ALEKSEEVA, ANISIMOV e RYZHENKOV, «Environmental terrorism», cit., p. 24.

⁵³ Doravante, as referências a eco-terrorismo estarão relacionadas tão-somente com a segunda definição desenvolvida anteriormente e que é, de facto, o objecto de análise do presente artigo.

⁵⁴ MESTRE, «Segurança ambiental e terrorismo», cit., p. 18, apresenta exemplos hipotéticos demonstrativos de como actos terroristas ambientais poderiam afectar diversas comunidades humanas e as suas actividades económicas. Estes não serão, naturalmente, incluídos aqui por não representarem situações reais.

3.2. Registos de eco-terrorismo

Um dos primeiros exemplos conhecidos de terrorismo ecológico moderno assumiu a forma de terrorismo de Estado⁵⁵. Entre 1962 e 1971, forças militares dos Estados Unidos da América disseminaram uma mistura de herbicidas conhecida como agente laranja (*agent orange*) no Vietname com o duplo objectivo de desfolhar as zonas de floresta onde se poderiam esconder forças vietnamitas e destruir áreas de cultivo que alimentariam as populações locais. Este agente químico consiste num conjunto de ácidos e produtos tóxicos altamente corrosivos. Cerca de 50 milhões de litros foram dispersados por meios aéreos a voar a baixa altitude, juntamente com outros químicos⁵⁶. Para além dos danos ambientais graves e duradouros, também se acredita que a elevada taxa de malformações e de doenças nas populações locais durante a década de 70 – como abortos espontâneos, cancro, deficiências congénitas nos nascituros e doenças dermatológicas – seja resultado da exposição a estes agentes químicos⁵⁷.

Outro caso, recordado por Heger mas sobejamente conhecido, consistiu na destruição de centenas de campos de exploração petrolífera no Kuwait por tropas talibás sob o comando de Saddam Hussein, em Fevereiro de 1991, durante a denominada segunda guerra do Golfo⁵⁸. Os campos arderam durante cerca de nove meses⁵⁹, causando níveis de poluição muito elevados e sendo este considerado um dos maiores desastres ambientais de sempre⁶⁰. Esta foi a resposta à entrada no país da coligação internacional

⁵⁵ Outras referências poderiam ser feitas, como o caso de as tropas romanas salgarem os campos de Cartago ou a política soviética de queimar as terras por onde poderiam passar os combatentes Nazi para que não se pudessem alimentar (a este propósito, veja-se, em geral, ALVIN TOFFLER e HEIDI TOFFLER, *War and anti-war: Survival at the dawn of the 21st century*, 1993, Boston). Não obstante, este texto foca-se numa realidade mais recente, nomeadamente a partir da segunda metade do século XX, desde logo pelo surgimento da nomenclatura associada ao terrorismo.

⁵⁶ Todos com o nome da cor pintada nos seus bidões, nomeadamente azul, branco, púrpura, rosa e verde.

⁵⁷ Encyclopaedia Britannica, *Agent Orange*, 20 de novembro de 2017 (acesso em 5 de Junho de 2019).

⁵⁸ HEGER, «Terrorist attacks against the natural environment», cit., p. 1072.

⁵⁹ SEBASTIÃO SALGADO, *When the oil field burned*, 1 de Agosto de 2016 (acesso em 4 de Junho de 2019).

liderada pelos Estados Unidos da América para combater o terrorismo na região, partilhando muitas características tanto de conflitos armados como de eco-terrorismo.

Existem igualmente duas situações que se deram fora de um contexto de conflito armado e que não são consensualmente classificadas pela doutrina como eco-terrorismo. Aliás, O’Lear chega a utilizar o segundo caso para questionar a definição desta variante de terrorismo, visto que a largueza do conceito de ambiente pode diminuir a precisão da definição e complicar a legiferação. O primeiro caso teve lugar em Janeiro de 1995. Um grupo de pescadores armados invadiram a estação de investigação Darwin nas ilhas Galápagos e fizeram dezenas de cientistas reféns em retaliação contra a proibição de pesca de pepinos-do-mar. Apesar das forças armadas do Equador terem conseguido dominar a situação sem vítimas humanas, foi mais tarde descoberto que os pescadores tinham torturado, mutilado e morto cerca de 81 tartarugas para pressionar os cientistas e o governo local⁶¹. A segunda situação ocorreu em Julho de 2000. 153 trabalhadores que haviam sido despedidos da fábrica de têxteis *Cellatex*, em *Givet*, levaram a cabo o que seria denominado o primeiro caso de terrorismo eco-industrial em França⁶² ao derramarem cerca de 5 600 litros de ácido sulfúrico num canal que desemboca no rio Meuse. Segundo alegavam, esta seria a primeira de quatro acções terroristas que culminariam na destruição do complexo industrial e que teriam como objectivo exigir melhores condições remuneratórias pelo seu despedimento⁶³.

Mais recentemente, ficou conhecido o já referido ataque à estação hidroeléctrica de *Baksan*, na Rússia, e vieram a público, em 2018 e 2019, notícias sobre a política israelita de não sancionar os colonizadores que têm vindo a destruir campos agrícolas e oliveiras nas zonas de ocupação. Muitas vezes os militares participam nos ataques ou apenas assistem à vandalização das quintas sem deterem os criminosos, que têm como objectivo instigar

⁶⁰ GILBERTO CRUZ, *Top 10 environmental disasters*, 2 de Maio de 2010 (acesso em 4 de Junho de 2019).

⁶¹ SCHWARTZ, «Environmental terrorism», cit., pp. 489-490.

⁶² CHALECKI, «A new vigilance», cit., p. 54.

⁶³ Independent, *France caves into workers who put acid in river*, 21 de Julho de 2000 (acesso em 20 de Agosto de 2019).

o medo nas populações palestinianas locais e forçá-las a abandonar a região. É um tipo de terrorismo muito particular que, na verdade, «has long since become routine in the West Bank»⁶⁴ e que conta com a conivência da polícia e de outras autoridades israelitas. É um terrorismo ambiental e económico, pois que os recursos e bens ambientais destruídos são essenciais à economia local. Apesar de não haver casos registados de violência contra as populações relacionados com estes ataques terroristas, isto tem tido o efeito psicológico de terror pretendido e os danos ambientais são graves. De facto, tal tem «essentially erected invisible walls throughout the West Bank, which Palestinians know crossing will expose them to violence and even danger to their lives»⁶⁵.

A última situação a registar – até 2019, entenda-se – foi a tensão entre a Índia e o Paquistão sobre a destruição parcial do campo florestal de *Balakot*, com que se iniciou este texto. Apesar de serem poucos os casos inequívocos de terrorismo ambiental, e considerando que não é líquida a referência a eco-terrorismo em situações de conflito armado, é importante recordar, desde logo, que quase todos os ataques terroristas, independentemente da sua natureza e características, têm um impacto no meio ambiente que deveria ser melhor conhecido e debatido. Aliás, quase todos os atentados poderiam ser categorizados, de uma forma ou de outra, como eco-terrorismo, ressaltando a intensidade dos danos.

Em todo o caso, o tratamento a que tem sido votado o ambiente nas discussões sobre terrorismo e na legislação internacional é insuficiente em face das consequências severas que podem resultar deste tipo de ataques. Há um vazio jus-internacional pois que os actos desta natureza até podem ser classificados como algum tipo de terrorismo e até podem ser sancionados internamente mas não tendem a ser encarados como terrorismo ecológico para o Direito e comunidade internacionais. O dano ao ambiente até poderá ser uma preocupação que decorre incidentalmente das circunstâncias mas não tem sido bastante para justificar legiferação ou a criação de políticas específicas a nível transnacional.

⁶⁴ The Israeli Information Center for Human Rights in the Occupied Territories, *Settlers destroy 2,000+ Palestinian-owned trees and vines, backed by Israeli authorities*, 5 de Agosto de 2018 (acesso em 22 de Agosto de 2019).

⁶⁵ *Id.*

A verdade é que, conforme escreveu Mestre, os estudos e políticas de segurança tendem a focar-se em ameaças que são prováveis de ser executadas e agentes que tenham a intenção e a capacidade de as concretizar. A aplicação destes critérios ao terrorismo ambiental permite compreender tanto o escasso número de casos de eco-terrorismo *proprio sensu* como a sua pouca vulgarização na literatura e nos meios de comunicação social. Os sistemas ambientais *per se* não parecem apresentar um interesse social e geopolítico suficiente para as organizações terroristas, que preferem atingir directamente alvos humanos e materiais não naturais para levar a cabo as suas agendas criminosas. Por outro lado, mesmo havendo danos ambientais, não parece existir interesse em sancioná-los de modo particular, *i.e.*, dissociado do restante dano. No entanto, o risco e os efeitos para o ambiente do terrorismo são demasiado sérios para que persista uma ausência de enquadramento legal e para que continuem lateralizados. Há uma atitude generalizada de indiferença em relação ao impacto ambiental do terrorismo que, naturalmente, acaba por afectar a noção e a percepção do eco-terrorismo – e que é mister alterar.

3.3. A legislação internacional actual

Apesar de a categoria de terrorismo ambiental ser, por ora, pouco mais do que uma construção doutrinal, a verdade é que os danos ao ambiente deveriam ser relevados a nível da consciência da comunidade internacional para que este termo passe a ser comum nos discursos institucionais mundiais quando se fala do fenómeno e da luta global contra o terrorismo. Mesmo que não chegue a ser um tipo de crime *tout court*, conviria que o ambiente fosse elevado ao estatuto de bem jurídico a proteger, em toda a linha.

Nenhum dos 19 protocolos e convenções adoptados desde 1963 pelas Nações Unidas para combater o terrorismo tem como objectivo directo e claro a protecção do meio ambiente. É preciso procurar por documentos que protejam o ambiente em caso de acções criminosas ou ilegítimas, sendo que a maior parte dos textos respeitam a situações de guerra ou conflito armado. Sem preocupações de exaustividade conceptual, e tal como desde início, serão aqui incluídas como terroristas também as acções levadas a cabo por Estados e forças (para)militarizadas, seja em contextos pacíficos ou em

cenários de confronto, que tenham contornos materiais semelhantes ao terrorismo praticado por agentes não estatais e que se poderiam também classificar como uso ilegítimo da força.

A primeira referência codificada de protecção do meio ambiente contra actos criminosos (potencialmente terroristas, embora a expressão não seja usada) consta do Tratado para a Antártida de 1959⁶⁶. Logo o n.º 1 do artigo 1.º prevê que a “Antártida será usada exclusivamente para fins pacíficos”, sendo proibidas quaisquer medidas de natureza militar e ensaios de armas. Tal é reforçado pelo artigo 5.º, cujo n.º 1 dispõe que serão proibidas a «realização de explosões nucleares ou a eliminação de resíduos de materiais radioactivos» na região.

Na mesma lógica, o Tratado de proibição parcial de testes nucleares⁶⁷ também protege o meio ambiente contra testes que poderiam ser usados, nomeadamente, como pressão geopolítica e, quiçá, terrorismo de Estado. No número 1 do n.º 1.º prevê-se que os Estados proibam, previnam e não encetem testes por intermédio de explosões de armas nucleares nos territórios sob sua jurisdição ou controlo, sendo que no número seguinte as Partes comprometem-se a não causar, encorajar ou, de algum modo, participar nesses testes ou na detonação de material nuclear. A referência, na alínea a) do n.º 1, a todo o tipo de ambientes naturais – atmosfera, espaço exterior e área marítima – pode ser interpretada como um acautelar de todos os ecossistemas contra os danos que poderão advir das explosões com armas nucleares.

Em 1972, é aberta a porta para a produção de legislação internacional de combate ao terrorismo que vise o meio ambiente. Apesar de não se utilizar a expressão terrorismo, nos termos do princípio 22 da Declaração da Conferência das Nações Unidas sobre o meio ambiente humano⁶⁸, também conhecida como Declaração de Estocolmo, «States shall cooperate

⁶⁶ Tratado para a Antártida, assinado em Washington a 1 de Dezembro de 1959 e em vigor desde 23 de Junho de 1961.

⁶⁷ *Treaty banning nuclear weapon tests in the atmosphere, in outer space and under water (Partial test ban treaty)*, assinado em Moscovo a 5 de Agosto de 1963 e em vigor desde 10 de Outubro de 1963.

⁶⁸ Declaração da Conferência das Nações Unidas sobre o meio ambiente humano, reunida em Estocolmo de 5 a 16 de Junho de 1972.

to develop further the international law regarding liability and compensation for the victims of pollution and other environmental damage caused by activities within the jurisdiction or control of such States to areas beyond their jurisdiction». O princípio 26 prevê ainda que «[m]an and his environment must be spared the effects of nuclear weapons and all other means of mass destruction».

Nesse mesmo ano, entrou em vigor o Tratado que proíbe a colocação de armas nucleares no leito marinho⁶⁹. Tal como o diploma que proíbe os testes nucleares, também se pode retirar do seu articulado que as proibições de colocação destas armas no leito marinho pretendem proteger este ambiente natural contra incidentes ou usos ilegítimos, terrorismo incluído. O n.º 1 do artigo 1.º admoesta os Estados a:

Not to emplant or emplace on the seabed and the ocean floor and in the subsoil thereof beyond the outer limit of a sea-bed zone (...) any nuclear weapons or any other types of weapons of mass destruction as well as structures, launching installations or any other facilities specifically designed for storing, testing or using such weapons.

Por outro lado, o artigo 5.º compraz uma disposição singular, como que aconselhando as Partes «to continue negotiations in good faith concerning further measures in the field of disarmament for the prevention of an arms race on the sea-bed, the ocean floor and the subsoil thereof». Apesar de se dirigir às Partes contratantes, o dever aqui inscrito pode ser interpretado como estendendo-se a um controlo sobre agentes e actividades terroristas que se estejam a desenvolver nos seus respectivos territórios.

Uma outra referência que ver com cuidados relativos ao ambiente natural consta do artigo 2.º da Convenção sobre armas bacteriológicas ou tóxicas de 1975⁷⁰, que urge cuidado no manuseio de armas biológicas. Aí se diz que:

⁶⁹ *Treaty on the prohibition of the emplacement of nuclear weapons and other weapons of mass destruction on the sea-bed and the ocean floor and in the subsoil thereof*, assinado em Londres, Moscovo e Washington a 11 de Fevereiro de 1971 e em vigor desde 18 de Maio de 1972.

⁷⁰ Convenção sobre a proibição do desenvolvimento, da produção e do armazenamento das armas bacteriológicas (biológicas) ou tóxicas e sobre a sua destruição, assinada em Washington a 29 de Junho de 1972 e em vigor desde 26 de Março de 1975.

Cada Estado Parte (...) compromete-se a destruir ou a desviar para fins pacíficos, tão depressa quanto possível (...), todos os agentes, toxinas, armas, equipamentos e vectores (...) que se encontram na sua posse ou sob a sua jurisdição ou controle. Quando da execução das disposições do presente artigo, haverá que tomar todas as precauções necessárias para proteger as populações e o meio ambiente.

No ano seguinte foi dado um passo importante, sendo a protecção do meio natural contra ingerências ilegais prevista na comumente designada por Convenção de Genebra sobre a modificação das condições ambientais⁷¹. Trata-se aqui de situações de terrorismo de Estado⁷², sendo que, no artigo 1.º, os Estados signatários comprometem-se «not to engage in military or any other hostile use of environmental modification techniques having widespread, long-lasting or severe effects as the means of destruction, damage or injury». O artigo seguinte explica que estas técnicas de modificação são «any technique for changing – through the deliberate manipulation of natural processes – the dynamics, composition or structure of the earth, including its biota, lithosphere, hydrosphere and atmosphere, or of outer space». Esta convenção é direccionada, sobretudo, a Estados beligerantes que possam afectar os recursos naturais como manobra de pressão ilegítima para obter resultados mais favoráveis no confronto militar. É de lamentar, porém, não haver a descrição do processo aplicável a quem desrespeitar estes trâmites e que a Convenção não incluía terrorismo não estatal de forma explícita⁷³.

Em 1977, a protecção ambiental contra consequências de conflitos armados saíria reforçada com um protocolo adicional a outras convenções de Genebra, desta feita as de 1949. Na secção dos métodos e meios de guerra⁷⁴,

⁷¹ *Convention on the prohibition of military or any other hostile use of environmental modification technique*, assinada em Nova Iorque a 10 de Dezembro de 1976 e em vigor desde 5 de Outubro de 1978.

⁷² Muito embora se possa considerar, com legitimidade, que seja somente designado como uso ilegítimo da força e um caso de violação das leis bélicas e não uma situação de terrorismo (SCHWARTZ, «Environmental terrorism», cit., p. 491).

⁷³ O'LEAR, «Environmental terrorism», cit., p. 142.

⁷⁴ Protocolo I adicional às Convenções de Genebra de 12 de Agosto de 1949 relativo à protecção das vítimas dos conflitos armados internacionais, aprovado em Genebra a 8 de Junho

em particular no nº 3 do artigo 35.º, é garantida como regra fundamental a proibição de «utilizar métodos ou meios de guerra concebidos para causar, ou que se presume irão causar, danos extensos, duráveis e graves ao meio ambiente natural». Novamente está-se perante uma situação que tanto se pode classificar como acção ilegítima em conflito armado como de terrorismo de Estado, dependendo da amplitude da interpretação. Seja como for, importa referir estes casos aqui para se ter uma visão mais global de uma realidade em construção. Já o artigo 55.º é das normas mais explícitas de protecção da natureza em Direito Internacional e poderá servir como modelo para articulados futuros que se debrucem sobre o eco-terrorismo. Epigrafado «protecção do meio ambiente natural», o seu nº 1 dispõe que:

A guerra será conduzida de forma a proteger o meio ambiente natural contra danos extensivos, duráveis e graves. Esta protecção inclui a proibição de utilizar métodos ou meios de guerra concebidos para causar ou que se presume venham a causar tais danos ao meio ambiente natural, comprometendo, por esse facto, a saúde ou a sobrevivência da população.

O nº 2 acrescenta que «[s]ão proibidos os ataques contra o meio ambiente natural a título de represália». Releva aqui apontar para o facto de que o elemento final humano pode enviesar a protecção jurídica presente na norma que se extrai do nº 1. É que, enquanto que a primeira frase autonomiza o meio ambiente das populações humanas, já a segunda parece tornar dependente a proibição de usar determinados meios bélicos do comprometimento da «saúde ou [d]a sobrevivência da população». Não é claro que esta segunda frase seja uma cláusula interpretativa da primeira, sendo que a primeira parece ser mais ampla do que a segunda. Mas, a ser, não estará salvaguardada a protecção devida ao meio ambiente em situações de guerra; assim se inquinando a defesa da natureza, ligando-a necessariamente aos seres humanos. Se, *a contrario*, os redactores tenham querido sublinhar a importância do ambiente, sendo os danos humanos um critério de censurabilidade adicional, a formulação não terá sido particularmente feliz.

de 1977 e em vigor desde 7 de Dezembro de 1978. Há igualmente um segundo e terceiro protocolos mas não abordam estas matérias.

Um texto singular que igualmente respeita à protecção do ambiente contra actividades humanas ilegais é o Acordo sobre as actividades dos Estados na Lua e outros corpos celestes⁷⁵. O n.º 1 do artigo 3.º é semelhante ao n.º 1 do artigo 1.º do Tratado para a Antártida, aí se prevendo que a Lua será usada pelos Estados contratantes para fins exclusivamente pacíficos, sendo proibidas quaisquer ameaças ou uso da força e acções hostis (ou ataques) contra a Lua, nos termos do n.º 2. A Lua igualmente não deverá ser usada para se cometerem actos ou ameaças contra a Terra, a própria Lua ou objectos espaciais humanos. Para além disso, o n.º 3 consagra que os Estados não deverão colocar nem usar armas nucleares ou outros tipos de armas de destruição maciça na órbita ou na superfície deste corpo celeste. Igualmente são ilegais os testes de qualquer tipo de arma e as manobras militares neste satélite, segundo o n.º 4 do mesmo preceito.

No ano seguinte, em 1980, foi assinada uma Convenção que versa sobre os efeitos de certas armas convencionais nos seres humanos⁷⁶. No entanto, quase ironicamente, o último número do último artigo do último protocolo adicional que seria assinado em simultâneo com esta Convenção é que prevê uma proibição expressa de provocação de danos ao meio ambiente⁷⁷. Diz o n.º 4 do seu artigo 2.º que é «proibido submeter florestas e outros tipos de cobertura vegetal a ataques com armas incendiárias, excepto quando esses elementos naturais são utilizados para cobrir, dissimular ou camuflar os combatentes ou outros objectivos militares ou são eles próprios os objectivos militares». É verdade que esta não é uma situação propriamente de terrorismo nem se apresenta como significativa protecção devido à excepção que se apresenta na segunda parte do trecho. Não obstante, é uma previsão que deverá impedir danos significativos ao meio ambiente de forma ilegítima e que poderão mesmo resultar de terrorismo de Estado, dependendo da casuística das situações⁷⁸.

⁷⁵ *Agreement governing the activities of States on the Moon and other celestial bodies*, assinado em Nova Iorque a 5 de Dezembro de 1979 e em vigor desde 11 de Julho de 1984.

⁷⁶ Convenção sobre a Proibição ou Limitação do Uso de Certas Armas Convencionais que Podem Ser Consideradas como Produzindo Efeitos Traumáticos Excessivos ou Ferindo Indiscriminadamente, assinada em Genebra a 10 de Outubro de 1980 e em vigor desde 2 de Dezembro de 1983.

⁷⁷ Protocolo sobre a proibição ou limitação do uso de armas incendiárias (Protocolo III), assinado em Genebra a 10 de Outubro de 1980 e em vigor desde 2 de Dezembro de 1983.

Dois anos volvidos e seria dado um passo bastante significativo com a Carta Mundial para a Natureza⁷⁹. Embora não seja vinculativo, este documento demonstra um consenso de várias nações em afirmar alguns princípios de conservação e defesa que devem reger «*all human conduct affecting nature*», como se diz no considerando c) do seu preâmbulo. Parece plausível afirmar que são princípios a ter em conta também quando se avalie a prática de actos de terrorismo que afectem o meio natural.

Seria este, aliás, outro bom ponto de partida para se legislar concretamente sobre o eco-terrorismo e as medidas de combate a este fenómeno. O primeiro princípio, constante do nº 1 do artigo 1.º, consiste no respeito pela natureza e na proibição de impedimento dos seus processos essenciais. O nº 2 adianta que «*the population levels of all life forms, wild and domesticated, must be at least sufficient for their survival, and to this end necessary habitats shall be safeguarded*». A criminalidade, em geral, e o terrorismo, em particular, não deverão destruir as formas de vida existentes no planeta nem o seu habitat natural. O nº 3 estende esta lógica ao meio abiótico, consagrando que «*[a]ll areas of the earth, both land and sea, shall be subject to these principles of conservation*». E, finalmente, o princípio mais claro no que concerne a práticas de terrorismo consta do nº 5. Aqui, há, pela primeira vez dirigida a todos os actores da comunidade internacional, uma proibição de afectar o ambiente com práticas criminosas ou abusivas, estando escrito que a natureza «*shall be secured against degradation caused by warfare or other hostile activities*».

Esta premissa é reforçada pelo disposto nos artigos 20.º e 21.º, sendo que o primeiro urge a que se evitem todas as actividades militares que danifiquem o ambiente e a alínea d) do segundo admoesta os «*States and, to the extent they are able, other public authorities, international organizations, individuals, groups and corporations [to ensure] that activities within their jurisdictions or control do not cause damage to the natural systems located within other States or in the areas beyond the limits of national jurisdiction*». Para além

⁷⁸ Basta recordar o primeiro exemplo dado na secção anterior, nomeadamente das forças militares Norte-Americanas, entre 1962 e 1971, terem disseminado litros de agente laranja nas florestas vietnamitas.

⁷⁹ *World Charter for Nature*, aprovada pela Assembleia Geral das Nações Unidas a 28 de Outubro de 1982 na sua 48.ª sessão plenária (Doc. A/RES/37/17).

disso, nos termos do artigo seguinte e de forma semelhante ao princípio 22 da Declaração de Estocolmo de 1972, os danos ao meio natural, obviamente incluídos aqueles produzidos em virtude de ataques terroristas, devem ser causa bastante para que «*[a]ll persons (...) have access to means of redress when their environment has suffered damage or degradation*».

A acrescentar ao que foi dito, a resolução de 25 de Novembro de 1992 da Assembleia Geral das Nações Unidas, respeitante à protecção do ambiente em situação de conflito armado, apelou a que os Estados tomassem todas as medidas necessárias para cumprirem com o Direito Internacional que protege o meio ambiente em momentos bélicos, chamou à adesão aos relevantes instrumentos multilaterais para aqueles que ainda não o tivessem feito e pediu aos Estados que incorporassem as normas jus-internacionais de protecção do ambiente natural nos seus manuais militares. Tal como o primeiro Protocolo adicional às convenções de Genebra de 1949 e a Carta Mundial para a Natureza, este poderia ser um modelo interessante na criação de políticas e medidas legislativas internacionais de protecção do ambiente em caso de terrorismo, especialmente usando este último apelo à incorporação nos regimes jurídicos nacionais de normas internacionais que protejam o ambiente e promovam o desenvolvimento sustentável.

Apesar de tudo, somente em 1998 é que seria aprovado o primeiro documento internacional sobre terrorismo a prever expressamente os danos ao meio ambiente como variante autónoma deste tipo de crime. Nos termos do n.º 2 do artigo 1.º da Convenção Árabe para a Supressão do Terrorismo⁸⁰, o terrorismo pode ser «*[a]ny act or threat of violence, whatever its motives or purposes, that occurs in the advancement of an individual or collective criminal agenda and seeking (...) to cause damage to the environment*». A utilização da locução disjuntiva «ou» entre os tipos de bens que podem sofrer com estas práticas para efeitos desta Convenção demonstra que o ambiente é aqui tutelado *per se*, sem que ofensas a outros bens tenham de ser cumuladas com os danos ecológicos para se classificar o tipo objectivo de crime como terrorismo. Outro aspecto positivo a apontar é que o texto detalha modos

⁸⁰ *Arab Convention for the suppression of terrorism*, assinada no Cairo a 22 de Abril de 1998 e em vigor desde 7 de Maio de 1999.

de cooperação para o combate e supressão do terrorismo a tomar pelas Partes contratantes, muito embora não especifique medidas a considerar para cada tipo de contra-terrorismo em concreto. Em todo o caso, é um sinal significativo para a comunidade internacional de que é possível incluírem-se os danos ao ambiente como causa suficiente para classificar certa criminalidade como terrorismo.

Outro passo positivo foi dado imediatamente no ano seguinte, em que é aprovada uma convenção, de certo modo, próxima desta. A Convenção da Organização da Conferência Islâmica para Combater o Terrorismo Internacional⁸¹ define, nos termos do segundo parágrafo do seu artigo 1.º, que terrorismo «*means any act of violence or threat thereof notwithstanding its motives or intentions perpetrated to carry out an individual or collective criminal plan with the aim of (...) exposing the environment (...) to hazards or occupying or seizing [it], or endangering a national resource*». Os autores do texto parecem ter-se inspirado na Convenção árabe de 1998, sendo de notar, em especial, novamente o uso da locução «ou» para distinguir entre variantes de terrorismo dentro da definição geral, num sentido que parece equiparar o valor dos bens jurídicos a proteger, colocando em paridade, neste sentido, o ambiente e, por exemplo, as vidas humanas.

Novo avanço na consideração do ambiente como bem a tutelar será dado em 1999, desta feita perante o desenvolvimento de tecnologias nucleares. O artigo 1.º do Tratado de Cooperação entre os Estados-Membros da Comunidade de Estados Independentes para Combater o Terrorismo⁸² define como terrorismo tecnológico:

The use or threat of the use of nuclear, radiological, chemical or bacteriological (biological) weapons or their components, pathogenic micro-organisms, radioactive substances or other substances harmful to human health, including the seizure, putting out of operation or destruction of nuclear, chemical or other facilities posing an increased technological and environmental danger (...), if these acts are committed

⁸¹ *Convention of the Organisation of the Islamic Conference on combating international terrorism*, assinada em Uagadugu a 1 de Julho de 1999 e em vigor desde 7 de Novembro de 2002.

⁸² *Treaty on cooperation among the States Members of the Commonwealth of Independent States in combating terrorism*, assinado em Minsk a 4 de Junho de 1999 e em vigor nas ordens jurídicas internas desde a assinatura de cada Estado parte.

for the purpose of undermining public safety, terrorizing the population or influencing the decisions of the authorities in order to achieve political, mercenary or any other ends.

É de sublinhar que o perigo ambiental aqui previsto parece ser tido como um meio através do qual se causam danos a seres humanos. Não se considera o ambiente como bem jurídico autónomo a proteger caso venha a ser alvo de um ataque terrorista. Apesar desta visão antropocêntrica, imediatamente a seguir se definem como «*[f]acilities posing an increased technological and environmental danger [the] enterprises, installations, plant and other facilities whose inoperability may lead to (...) pollution of the environment*». Aqui sim há um cuidado em considerar como perigosas as indústrias que causem danos ambientais. Muito embora possa não ter valor juridicamente relevante, a colocação desta acepção a seguir às definições de terrorismo e terrorismo tecnológico permite, talvez, ler uma certa reflexão dos autores em agrupar o que considera serem as principais fontes de perigosidade e os bens jurídicos a ter em atenção. Por exemplo, parece plausível que tenham ponderado no uso destas instalações como meios para levar a cabo acções terroristas contra o ambiente já que o Tratado diz respeito, precisamente, ao combate ao terrorismo. Isto é reforçado pelo disposto nas alíneas e) e j) do nº 1 do artigo 5.º, que preveem que as autoridades competentes dos Estados signatários devem auxiliar-se mutuamente para avaliarem as condições físicas destas instalações perigosas e financiarem investigações científicas que permitam melhorar essas mesmas condições.

Um mês após a aprovação deste Tratado, seria adoptado um novo documento que, tal como as Convenções árabe e da Organização da Conferência Islâmica, prevê o terrorismo ambiental como uma categoria autónoma. Segundo a alínea a) do nº 3 do artigo 1.º da Convenção da Organização da União Africana sobre Prevenção e Combate ao Terrorismo⁸³, um acto terrorista significa «*any act which is a violation of the criminal laws of a State Party and which may endanger (...) or may cause damage to (...) natural resources [or] environmental (...) heritage*».

⁸³ *Organization of the African Union Convention on the prevention and combating of terrorism*, assinada em Argel a 14 de Julho de 1999 e em vigor desde 6 de Dezembro de 2002.

Esta é, porém, uma formulação bastante específica e aquém do alcance dos referidos textos por duas razões. Em primeiro lugar, remete para Direito interno a definição e criminalização de actos terroristas, seja de terrorismo ambiental ou de outra natureza. Daqui resulta, em concreto, que o eco-terrorismo – que já de si não tem significativa expressão no ordenamento jurídico global – não só não está consagrado nesta Convenção de forma expectável como nem sequer será uma realidade tutelada nos territórios das Partes contratantes se estas não o previrem autonomamente em legislação nacional. É verdade que, na alínea a) do artigo 2.º, os Estados se comprometem a «*review their national laws and establish criminal offences for terrorist acts as defined in this Convention and make such acts punishable by appropriate penalties that take into account the grave nature of such offences*». No entanto, não deixa de haver aqui um elemento de aleatoriedade pois que é dada uma ampla margem de discricionariedade aos Estados, assumindo sequer que o farão. Em rigor, estas normas, bem como a sua execução e força jurídica, tornam-se reféns de preceitos nacionais que poderão estar longe de punições justas e de um tratamento humano e adequado – uma espécie de ‘sequestro’ que nem sequer tem como resposta a aplicação de sanções pelo não cumprimento.

Em seguida, é de apontar que, em vez de se ter escrito genericamente que seriam actos terroristas aqueles que provocassem danos ou ameaçassem o ambiente ou a natureza, as Partes preferiram os termos concretos de «recursos naturais» e «herança ambiental». Uma interpretação hermenêutica mais rigorosa deve concluir que tais expressões diminuem sensivelmente a abrangência da norma, deixando de fora os ambientes naturais que não representem um interesse económico ou produtivo (ou seja, não sejam recursos naturais) e aqueles que não tenham uma carga cultural, histórica ou singular de relevo (como locais de interesse natural declarados como tal pelas Nações Unidas). Donde, é possível que ataques terroristas que causem graves danos ao ambiente não sejam censurados pela comunidade de Estados contratantes porque afectam o ambiente tido como banal.

Para além disso, dispõe o nº 1 do artigo 3.º que a «*struggle waged by peoples in accordance with the principles of international law for their liberation or self-determination, including armed struggle against colonialism, occupation, aggression and domination by foreign forces shall not be considered as terrorist acts*» e, o nº 2, que «*[p]olitical, philosophical, ideological, racial, ethnic, religious*

or other motives shall not be a justifiable defence against a terrorist act». Não há espaço para aprofundar, mas parece que estes preceitos são cartas abertas a atentados terroristas que podem lesar significativamente o meio ambiente e que poderão passar sem qualquer sanção.

Já neste século, o parágrafo iv) da alínea b) do nº 2 do artigo 8.º do Estatuto do Tribunal Penal Internacional⁸⁴ determina, entre outros, que crimes de guerra serão todas as «violações graves das leis e costumes aplicáveis em conflitos armados internacionais no quadro do direito internacional», nomeadamente ataques que causem «prejuízos extensos, duradouros e graves no meio ambiente que se revelem claramente excessivos em relação à vantagem militar global concreta e directa que se previa». Como defende Heger⁸⁵, não há aqui uma genuína ligação ao crime de terrorismo. Um ataque militar organizado no âmbito de um conflito armado internacional que cause danos ao ambiente ou que recorra a armas químicas ou biológicas⁸⁶ não se considera como um acto de terrorismo, no entender deste autor, mesmo que se lhe assemelhe materialmente. Os exércitos e as políticas de guerra não têm, *prima facie*, o escopo de causar terror nos mesmos termos que os agentes comumente designados por terroristas. No entanto, o autor reconhece que há grupos terroristas que se comportam e têm capacidades bélicas semelhantes a milícias ou mesmo a certos exércitos. Aliás, algumas práticas serão mesmo de difícil categorização, encontrando-se numa zona cinzenta entre actividades militares abusivas e terrorismo ecológico, como se viu no caso da destruição dos campos de exploração petrolífera, em 1991, no Kuwait. É esta indefinição que pode permitir alargar as acções ilegais para o campo do terrorismo do Estado, nem que seja para valorizar a importância do ambiente nesta matéria.

Mais recentemente, a Convenção Internacional para a Eliminação de Actos de Terrorismo Nuclear⁸⁷ deu mais um passo importante ao prever ex-

⁸⁴ Estatuto do Tribunal Penal Internacional, assinado em Roma a 17 de Julho de 1998 e em vigor desde 1 de Julho de 2002.

⁸⁵ HEGER, «Terrorist attacks against the natural environment», cit., p. 1071.

⁸⁶ Veja-se, não obstante, a nota de rodapé 37 em que se refuta o uso destas armas como critério necessário para se estar perante eco-terrorismo.

⁸⁷ Convenção Internacional para a Eliminação de Actos de Terrorismo Nuclear, assinada em Nova Iorque a 13 de Abril de 2005 e em vigor desde 7 de Julho de 2007.

pressamente uma tutela dos danos causados deliberadamente ao ambiente. Começa por definir, segundo o disposto no seu artigo 1.º, que material radioactivo é aquele que pode causar, entre outros, danos consideráveis no ambiente (nº 1) e que engenho é algo que, «devido às suas propriedades radiológicas», pode provocar o mesmo tipo de danos consideráveis (alínea b) do nº 4). No artigo seguinte, completa-se o quadro normativo ao considerar-se que é responsável por cometer uma infracção quem, ilícita e intencionalmente, detiver materiais radioactivos ou fabricar ou detiver engenhos com intenção de provocar danos consideráveis ao ambiente (item ii) da alínea a)) e quem, com a mesma intenção, empregar ou utilizar esses materiais ou engenhos ou causar danos numa instalação nuclear que levem à libertação ou risco de libertação de materiais radioactivos (item ii) da alínea b)). Tal como alguns textos anteriores, é de sublinhar que o dano ao ambiente é tutelado autonomamente, desbravando caminho para a repressão significativa do terrorismo ecológico. Ademais, não deve ser obstáculo serem Estados as Partes contratantes pois que as normas parecem dirigir-se a qualquer pessoa ou entidade que fabrique, detenha, empregue ou use este tipo de materiais perigosos.

Ainda quanto ao dano, e já em oposição àqueles outros documentos, deve ser ponderado o facto de se exigirem «danos consideráveis» para que haja a comissão de uma infracção punível nos termos desta Convenção. Esta expressão tem sido utilizada ao longo deste artigo muito a partir deste trecho, embora não seja possível quantificar à partida o que significa e quanto significa este critério. Não obstante, o terrorismo está de tal forma presente no contexto sociológico do intérprete-julgador que não deverá ser difícil encontrar ferramentas interpretativas, baseadas na própria experiência ou como resultado de situações análogas a partir de crimes com traços semelhantes, para determinar a suficiência dos danos no caso concreto.

4. (In)suficiente protecção legal

Da breve revista dos diplomas parece transparecer um certo desfasamento entre as crescentes preocupações ambientais da comunidade internacional e a regulação jurídica do terrorismo. Aliás, mesmo quando o ambiente é tutelado e a sua preservação aparenta ser uma das inquietações das Partes contratantes, como sucede distintamente nos tratados sobre armas nucleares,

raramente é dito de forma clara e explícita, quer nos articulados quer nos preâmbulos, que a ameaça ambiental é um dos objectivos a precaver com a regulação. Não há uma reflexão sobre os danos e as consequências nefastas sobre o meio ambiente nem há uma afirmação inequívoca de que estes acordos internacionais poderão servir também para preservar o ambiente natural da acção terrorista dos seres humanos.

A acrescer a isto, são pontuais os textos internacionais que tratam de forma particular a vertente do eco-terrorismo aqui analisada, adicionando explicitamente os danos ao ambiente nas suas definições de terrorismo, e ainda mais escassos os que preveem sanções à produção de danos ao ambiente ou que constroem um regime de contra-terrorismo. Isto não abona a favor da causa ambiental, existindo um défice legal e de política pública, por exemplo, quanto à actuação oficial em caso de ataques ao meio natural ou em que este seja danificado de forma relevante em virtude de práticas terroristas, como se potencialmente terá verificado na tensão entre a Índia e o Paquistão.

Parece até que os danos ambientais são insignificantes na contabilização das consequências do terrorismo, muito embora se verifiquem frequentemente. De facto, o ambiente sai quase sempre lesado após algum ataque, como dito anteriormente, e isto deveria ser tomado em consideração para uma protecção holística da natureza e para uma tutela eficiente e concertada de combate ao terrorismo.

Apesar de alguns estudos nas últimas décadas terem demonstrado uma certa ineficácia nos resultados do reforço das medidas de combate e dissuasão do terrorismo⁸⁸, há alguns textos internacionais que têm vindo a consagrar os danos ao ambiente na lógica do terrorismo e, mesmo, na de outras acções ilegais graves. Falta, assim, o passo decisivo de consagração de um pacote de medidas global, envolvendo cartas de princípios e resoluções da Assembleia Geral e do Conselho de Segurança das Nações Unidas, bem como acordos e convenções bilaterais ou multilaterais vinculativos, que torne o terrorismo ecológico visível e relevante no panorama jus-internacional. Não é desejável que se fique somente por instrumentos não vinculativos

⁸⁸ Vejam-se, em especial, as referências em CARSON e BARTHOLOMEW, «Terrorism outside the proverbial vacuum», cit., pp. 557-558.

ou meramente interpretativos nem parece razoável dizer que é preciso primeiro testar a adesão dos Estados a textos não vinculativos para depois, daqui a alguns anos, passar a textos com sanções efectivas. O tempo das experiências já passou e a protecção do ambiente é urgente também aqui.

De outro ponto de vista, da secção anterior resulta igualmente que a própria noção de terrorismo ambiental não tem sido desenvolvida de forma crítica pela doutrina. Tal poderá explicar, em parte, o pouco conhecimento deste fenómeno junto do público e das camadas políticas e, até mesmo, a falta de legislação. O’Lear perguntava-se, já em 2003, se haveria utilidade em estudar este sub-fenómeno para se compreender e teorizar sobre o terrorismo ou sequer se haveriam dados empíricos suficientes que valessem a pena investigações doutrinárias⁸⁹. Parece, porém, que, hoje em dia, o que é necessário é debater sobre se o bem jurídico ambiente deve ser visto, mesmo que numa capacidade simbólica, como um alvo (de relevo) do terrorismo e, portanto, merecedor de protecção específica por parte do Direito e das políticas contra-terroristas internacionais. Pegando ainda na análise daquele autor, será que as «*target audiences [of terrorism] may not be states but (...) tangible and non-tangible entities not ‘contained’ within fixed boundaries*»⁹⁰?

É, quiçá, menos importante enfatizar as táticas terroristas usadas do que o impacto no ambiente e recursos naturais em linha com uma *mens rea* criminosa para procurar uma definição sólida de terrorismo e para que não haja dúvidas em relação à inclusão do terrorismo ambiental na legislação e nas políticas internacionais. Apesar de complicar a classificação objectiva, esta segunda parte não deve ser descurada. Como exemplifica O’Lear, a destruição de florestas para fins económicos ou o depósito ilegal de lixo tóxico para evitar os custos de eliminação não têm «*the intention of communicating a message to a particular audience*»⁹¹, pelo que não devem ser vistos como actos eco-terroristas. Já a destruição ou contaminação propositada de áreas agrícolas ou fontes de água no sentido de lutar por uma determinada causa, nomeadamente de natureza política, deverá sim ser considerado como tal.

⁸⁹ O’LEAR, «Environmental terrorism», cit., p. 128.

⁹⁰ *Id.*, p. 135.

⁹¹ *Id.*, p. 136.

O quadro jus-internacional actual não basta para proteger o meio ambiente dos efeitos do terrorismo, seja ele direccionado contra o ambiente ou sendo este uma 'vítima' colateral. As definições mais divulgadas de terrorismo não tendem a incluir este aspecto, de forma algo contrária à complexificação deste fenómeno social⁹². Na verdade, o que deveria importar numa definição global, operacional e útil de eco-terrorismo são os danos que se podem reflectir no ambiente e a intenção criminosa. Só com este enfoque se poderá elevar o ambiente definitivamente à categoria de bem jurídico a tutelar e proteger, até contra comportamentos menos avisados dos Estados. Mas, como habitual, a vontade política será decisiva para que alguma vez isto suceda e para que o que é agora tão-somente uma categoria doutrinal passe a ser uma realidade de *lege data*.

A mutação do panorama jurídico internacional tende a ser complicada. Mas a verdade é que o terrorismo e, em especial, a violência de base religiosa e política têm vindo a aumentar, sendo que os danos que muitas vezes provocam tendem a superar a dimensão das organizações terroristas ou a sua aparente capacidade bélica, técnica e humana⁹³. Não será irrazoável pensar que o ambiente poderá tornar-se um alvo de relevo de chantagem terrorista no cenário actual de crescentes preocupações climáticas. Seria positivo, embora reconhecidamente pouco habitual, que legislação supra-nacional se 'adiantasse' a este fenómeno e o regulasse, fruto de uma vontade concertada da comunidade internacional em combater o terrorismo como meio de provocação de danos ao ambiente.

5. Conclusão

O aumento do *stress* ambiental e da fragilização dos meios e recursos naturais são factores de depleção do ecossistema global que colocam em risco a sustentabilidade da vida no planeta, tanto dos seres humanos como dos demais elementos bióticos. Daqui poderá resultar um ciclo perigoso, com decorrentes tensões sociais que incrementarão o risco de violência sob a forma de terrorismo e outra criminalidade grave e que, quiçá, por

⁹² O'LEAR, «Environmental terrorism», cit., p. 137.

⁹³ Veja-se, em geral, PETER CHALK, *Non-military security and global order: The impact of extremism, violence and chaos on national and international security*, Londres, 2000.

sua vez, poderão levar a uma maior «insegurança ambiental», como avisa Mestre⁹⁴.

Heger já alertou para o facto de que, apesar de o terrorismo contra o meio ambiente não ser uma realidade muito frequente na actualidade, há exemplos suficientes que justificam que se acautelem futuros ataques⁹⁵, especialmente à luz da consciência da fragilidade da natureza e da sua importância para a sobrevivência da espécie humana. De facto, o terrorismo ambiental pode tornar-se um dos desafios mais perigosos para a segurança internacional e para o desenvolvimento sustentável, sendo uma ameaça transversal a todos os países. Neste ponto, O’Lear recorda que todos os assuntos relacionados com o ambiente desafiam a visão tradicional de território no Direito Internacional. Se uma visão centrada nos Estados e nas suas fronteiras é desadequada para tratar de forma eficaz o fenómeno do terrorismo em sentido lato, ainda mais o é no que respeita ao terrorismo ambiental⁹⁶.

Nas palavras de Alekseeva, Anisimov e Ryzhenkov, a tecnologia hodierna que pode ir parar às mãos de grupos terroristas faz com que certas acções criminosas, por exemplo, contra indústrias nucleares, ponham em causa a vida humana e não-humana como a conhecemos. Tudo isto requer um estudo aprofundado do terrorismo ambiental, bem como o desenho de um pacote de medidas legais, sociais, políticas e económicas de antecipação e combate a este fenómeno⁹⁷. Pode dizer-se que esta chamada de atenção é a conclusão pragmática da questão conceptual e dogmática analisada neste artigo.

A literatura jus-internacional deve prestar mais atenção ao eco-terrorismo para que se consolide este tipo de crime na doutrina e nas políticas públicas, devendo começar por afinar a distinção entre delitos contra o ambiente e terrorismo ambiental, como menciona Heger⁹⁸. É importante dar a merecida relevância quer ao ambiente como bem jurídico que importa tutelar de forma autónoma quer aos danos que lhe são causados. Só assim se poderá recorrer aos meios institucionais de combate ao terrorismo transnacional e

⁹⁴ MESTRE, «Segurança ambiental e terrorismo», cit., pp. 24-25.

⁹⁵ HEGER, «Terrorist attacks against the natural environment», cit., p. 1073.

⁹⁶ O’LEAR, «Environmental terrorism», cit., p. 129.

⁹⁷ ALEKSEEVA, ANISIMOV e RYZHENKOV, «Environmental terrorism», cit., p. 33.

⁹⁸ HEGER, «Terrorist attacks against the natural environment», cit., p. 1073.

se fará com que a comunidade internacional trabalhe em conjunto para mitigar este flagelo.

Bibliografia

- Alekseeva, A., Anisimov, A. & Anatoliy, A., 2017. Environmental terrorism, environmental radicalism and measures to counteract them. *Environmental Policy and Law*, 47(1), pp. 24-34
- Amster, R., 2006. Perspectives on ecoterrorism: Catalysts, conflations, and casualties. *Contemporary Justice Review*, 9(3), pp. 287-301
- Balali-Mood, M., Moshiri, M. & Etemad, L., 2013. Medical aspects of bio-terrorism. *Toxicol*, 69, pp. 131-142
- Barber, M., 2019. *Pakistan to lodge UN complaint against India for 'eco-terrorism'*. Disponível em <https://www.jurist.org/news/2019/03/pakistan-to-lodge-un-complaint-against-india-for-eco-terrorism/#> [Acedido em 10 de Maio de 2019]
- Barsalou, O. & Picard, M. H., 2018. International environmental law in an era of globalized waste. *Chinese Journal of International Law*, 17, pp. 887-906
- BBC, 2018. *Tokyo Sarin attack: Japan executes last Aum Shinrikyo members on death row*. Disponível em <https://www.bbc.com/news/world-asia-44962581> [Acedido em 27 de Maio de 2019]
- Carson, J., 2014. Counterterrorism and radical eco-groups: A context for exploring the series hazard model. *Journal of Quantitative Criminology*, 30, pp. 485-504
- Carson, J. & Bartholomew, B., 2016. Terrorism outside the proverbial vacuum: Implications for the moral context. *Deviant Behavior*, 37(5), pp. 557-572
- Carson, J., LaFree, G. & Dugan, L., 2012. Terrorist and non-terrorist criminal attacks by radical environmental and animal rights groups in the United States, 1970–2007. *Terrorism and Political Violence*, 24(2), pp. 295-319
- Cary, S., 2009. The tipping point: Biological Terrorism. *Journal of Strategic Security*, 2(3), pp. 13-24
- Chalecki, E., 2002. A new vigilance: Identifying and reducing the risks of environmental terrorism. *Global Environmental Politics*, 2(1), pp. 46-64

- Chalk, P., 2000. *Non-military security and global order: The impact of extremism, violence and chaos on national and international security*. Londres: MacMillan Press
- Cooke, S., 2013. Animal rights and environmental terrorism. *Journal of Terrorism Research*, 4(2), pp. 26-35
- Cruz, G., 2010. *Top 10 environmental disasters*. Disponível em http://content.time.com/time/specials/packages/article/0,28804,1986457_1986501_1986442,00.html [Acedido em 4 de Junho de 2019]
- Dominelli, S., 2014. Evolutionary trends in maritime piracy: A possible assessment of eco-activists' conduct. *Australian International Law Journal*, 21, pp. 41-54
- Eagan, S., 1996. From spikes to bombs: The rise of eco-terrorism. *Studies in Conflict and Terrorism*, 19(1), pp. 1-18
- Encyclopaedia Britannica, 2019. *Agent Orange*. Disponível em <https://www.britannica.com/science/Agent-Orange> [Acedido em 5 de Junho de 2019]
- Foreman, D. & Haywood, B., 2002. *Ecodefense: A field guide to monkey-wrenching*. 3.^a edição. Chico: Abzug Press
- Freilich, J., Chermak, S. & Simone, J., 2009. Surveying American state police agencies about terrorism threats, terrorism sources, and terrorism definitions. *Terrorism and Political Violence*, 21(3), pp. 450-475
- Ganguly, G., Setzer, J. & Heyvaert, V., 2018. If at first you don't succeed: Suing corporations for climate change. *Oxford Journal of Legal Studies*, 38(4), pp. 841-868
- Greenpeace International, 2019. *Greenpeace turns world-famous 'Iamsterdam' landmark into solidarity message to save the Amazon*. Disponível em <https://www.greenpeace.org/international/press-release/22659/famous-iamsterdam-landmark-solidarity-message-amazon/> [Acedido em 23 de Agosto de 2019]
- Gruenewald, J., Allison-Gruenewald, K. & Klein, B., 2015. Assessing the attractiveness and vulnerability of eco-terrorism targets: A situational crime prevention approach. *Studies in Conflict & Terrorism*, 38(6), pp. 433-455
- Habermas, J., 2005. *The inclusion of the other: Studies in political theory*. Cambridge: Polity Press
- Heger, M., 2012. Terrorist attacks against the natural environment: A phantom or a real danger. *German Law Journal*, 13(9), pp. 1066-1074

- Hirsch-Hoefler, S. & Mudde, C., 2014. "Ecoterrorism": Terrorist threat or political ploy?. *Studies in Conflict & Terrorism*, 37(7), pp. 586-603
- Independent, 2000. *France caves into workers who put acid in river*. Disponível em <https://www.independent.co.uk/news/world/europe/france-caves-into-workers-who-put-acid-in-river-707730.html> [Acedido em 20 de Agosto de 2019]
- Joosse, P.,
2007. Leaderless resistance and ideological inclusion: The case of the Earth Liberation Front. *Terrorism and Political Violence*, 19(3), pp. 351-368
2012. Elves, environmentalism, and "eco-terror": Leaderless resistance and media coverage of the Earth Liberation Front. *Crime Media Culture*, 8(1), pp. 75-93
- Kellman, B., 2001. Biological terrorism: Legal measures for preventing catastrophe. *Harvard Journal of Law and Public Policy*, 24(417), pp. 425-488
- LaFree, G. & Dugan, L., 2007. Introducing the global terrorism database. *Terrorism and Political Violence*, 19, pp. 181-204
- Leamons, J., 2015. Eco-terrorism: A legal update on the laws protecting scientific research from extremist activists. *Journal of Biosecurity, Biosafety and Biodefense Law*, 6(1), pp. 23-42
- Liddick, D., 2006. *Eco-terrorism: Radical environmental and animal liberation movements*. Londres: Praeger
- Loadenthal, M.,
2013. Deconstructing "eco-terrorism": Rhetoric, framing and statecraft as seen through the Insight approach. *Critical Studies on Terrorism*, 6(1), pp. 92-117
2014. Eco-terrorism? Countering dominant narratives of securitisation: A critical, quantitative history of the Earth Liberation Front (1996-2009). *Perspectives on Terrorism*, 8(3), pp. 16-50
2016. Activism, terrorism, and social movements: The "green scare" as monarchical power. Em: L. Hancock (ed.), *Narratives of identity in social movements, conflicts and change*. Bingley: Emerald Group Publishing Limited, pp. 189-226
- Long, D., 2004. *Ecoterrorism*. Nova Iorque: Facts on File
- Lutherer, L. & Simon, M., 1993. *Targeted: The anatomy of an animal rights attack*. Oklahoma: University of Oklahoma Press

- Maroufi, C., 2018. *Salem Press Encyclopedia*. Nova Yorque: Salem Press
- Mestre, J., 2006. Segurança ambiental e terrorismo. *Revista Militar*, 2248, pp. 1-27
- Mueller, R., 2005. *Testimony*. Disponível em <https://archives.fbi.gov/archives/news/testimony/global-threats-to-the-u.s.-and-the-fbis-response-1> [Acedido em 24 de Maio de 2019]
- Nagtzaam, G., 2017. *From environmental action to ecoterrorism?: Towards a process theory of environmental and animal rights oriented political violence*. Cheltenham: Edward Elgar Publishers
- Nagtzaam, G. & Lentini, P., 2008. Vigilantes on the high seas?: The Sea Shepherds and political violence. *Terrorism and Political Violence*, 20, pp. 110-133
- O'Lear, S., 2003. Environmental terrorism: A critique. *Geopolitics*, 8(3), pp. 127-150
- Preston, A., 2012. Eco-terrorism in the southern ocean: A dangerous byproduct of the tangled web of international whaling conventions and treaties. *Whittier Law Review*, 34, pp. 117-139
- Reader, I., 2000. *Religious violence in contemporary Japan: The case of Aum Shinrikyo*. Richmond: Curzon
- Salgado, S., 2016. *When the oil field burned*. Disponível em <https://www.nytimes.com/interactive/2016/04/08/sunday-review/exposures-kuwait-salgado.html> [Acedido em 4 de Junho de 2019]
- Saul, B., 2008. *Defining terrorism in international law*. Oxford: Oxford University Press
- Sbârcea, C., Lerescu, L. & Jinga, M., 2014. Bio-terrorism: Still interesting or concerning nowadays?. *Romanian Journal of Military Medicine*, CXVII(3-4), pp. 5-10
- Scarce, R., 2016. *Eco-warriors: Understanding the radical environmental movement*. Nova Iorque: Routledge
- Schwartz, D., 1998. Environmental terrorism: Analyzing the concept. *Journal of Peace Research*, 35(4), pp. 483-496
- Shahzad, A., 2019. *Pakistan to lodge U.N. complaint against India for 'eco-terrorism' forest bombing*. Disponível em <https://www.reuters.com/article/us-india-kashmir-pakistan-environment/pakistan-to-lodge-u-n-complaint-against-india-for-eco-terrorism-forest-bombing-idUSKC N1QI4FX> [Acedido em 10 de Maio de 2019]

- Smith, R., 2008. “Ecoterrorism”?: A critical analysis of the vilification of radical environmental activists as terrorists. *Environmental Law*, 38, pp. 537-576
- Spier, J., 2018. The principles on climate obligations of enterprises: An attempt to give teeth to the universally adopted view that we must keep global warming below an increase of two degrees Celsius. *Uniform Law Review*, 23, pp. 319-335
- Sumner, D. & Weidman, L., 2013. Eco-terrorism or eco-tage: An argument for the proper frame. *Interdisciplinary Studies in Literature and Environment*, 20(4), pp. 855-876
- The Israeli Information Center for Human Rights in the Occupied Territories, 2018. *Settlers destroy 2,000+ Palestinian-owned trees and vines, backed by Israeli authorities*. Disponível em https://www.btselem.org/settler_violence/20180802_settlers_destroy_2000_palestinian_owned_trees [Acedido em 22 de Agosto de 2019]
- Tkachenko, M., 2010. *Power plant ‘terror’ attack kills 2 in Russia*. Disponível em <http://edition.cnn.com/2010/WORLD/europe/07/21/russia.station.attack/index.html> [Acedido em 27 de Maio de 2019]
- Toffler, A. & Toffler, H., 1993. *War and anti-war: Survival at the dawn of the 21st century*. Boston: Little Brown & Company
- Vanderheiden, S.,
2005. Eco-terrorism or justified resistance? Radical environmentalism and the “war on terror”. *Politics & Society*, 33(3), pp. 425-447
2008. Radical environmentalism in an age of antiterrorism. *Environmental Politics*, 17(2), pp. 299-318
- Villa, V., Reniers, G., Paltrinierie, N. & Cozzania, V., 2017. Development of an economic model for the allocation of preventive security measures against environmental and ecological terrorism in chemical facilities. *Process Safety and Environmental Protection*, 109, pp. 311-339
- Yang, S.-M. & Jen, I.-C., 2018. An evaluation of displacement and diffusion effects on eco-terrorist activities after police interventions. *Journal of Quantitative Criminology*, 34, pp. 1103-1123


O IX Encontro Luso-Espanhol de Professores de Direito Internacional e Relações Internacionais – IX Encuentro Luso- Español de Profesores de Derecho Internacional y Relaciones Internacionales, teve lugar em Lisboa, a 6 e 7 de junho de 2019, na Faculdade de Direito da Universidade de Lisboa, com o tema «O Direito Internacional e os Limites da Luta contra o Terrorismo – El Derecho Internacional y los Límites de la Lucha contra el Terrorismo». Foi organizado pelos Professores Doutores Maria Luísa Duarte e Fernando Loureiro Bastos, da Faculdade de Direito da Universidade de Lisboa e do Lisbon Public Law Research Centre/Centro de Investigação de Direito Público, e pelo Professor Doutor José Martín y Pérez de los Nanclares, da Faculdade de Direito da Universidade de Salamanca.




Lisbon
Public Law
Research Centre



 Faculdade de Direito de Lisboa
Alameda da Universidade, Lisboa

 livraria.aafdl.pt
ebooks.aafdl.pt

 217959379

