

TESIS DOCTORAL



UCAM

UNIVERSIDAD CATÓLICA
DE MURCIA

ESCUELA INTERNACIONAL DE DOCTORADO

Programa de Doctorado en Ciencias Sociales

El Agente Encubierto Informático como herramienta de
prevención del terrorismo yihadista

Autor/a:

D. Andrés Soriano Guillamón

Directores/as:

Dr. D. César Augusto Giner Alegría

Murcia, junio de 2025

TESIS DOCTORAL



UCAM

UNIVERSIDAD CATÓLICA
DE MURCIA

ESCUELA INTERNACIONAL DE DOCTORADO

Programa de Doctorado en Ciencias Sociales

El Agente Encubierto Informático como herramienta de
prevención del terrorismo yihadista

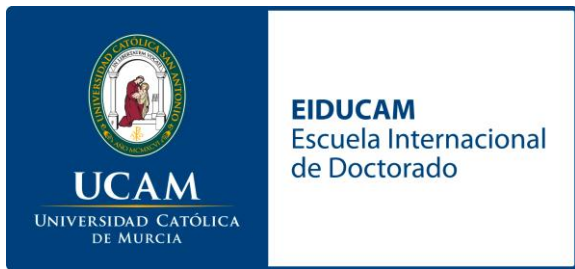
Autor/a:

D. Andrés Soriano Guillamón

Directores/as:

Dr. D. César Augusto Giner Alegría

Murcia, junio de 2025



AUTORIZACIÓN DEL DIRECTOR DE LA TESIS PARA SU PRESENTACIÓN

El Dr. D. César Augusto Giner Alegría como Director de la Tesis Doctoral titulada “El Agente Encubierto Informático como herramienta de prevención del terrorismo yihadista” realizada por D. Andrés Soriano Guillamón en el Programa de Doctorado en Ciencias Sociales, **autoriza su presentación a trámite** dado que reúne las condiciones necesarias para su defensa.

Lo que firmo, para dar cumplimiento al Real Decreto 99/2011 de 28 de enero, en Murcia a 01 de septiembre de 2025.

Firmado por CESAR AUGUSTO GINER ALEGRIA
- NIF:***2535** el día 30/09/2025 con un
certificado emitido por ACCVCA-120

Dr. D. César Augusto Giner Alegría.



RESUMEN

Hoy en día, el terrorismo yihadista se ha configurado como una de las amenazas globales más relevantes que enfrentan los gobiernos, no solo por sus efectos devastadores sobre la seguridad ciudadana, sino también por su rápida expansión a través del entorno digital. Desde el surgimiento en 2014 del autodenominado Califato Islámico de Daesh en Siria e Iraq, el ciberespacio se ha convertido en un espacio privilegiado para la captación, adoctrinamiento, financiación y difusión de propaganda terrorista, generando una radicalización violenta sustentada en una interpretación extremista del islam. Plataformas digitales como redes sociales, foros clandestinos y canales cifrados han potenciado una propaganda sofisticada capaz de embaucar a miles de adeptos dispuestos a perpetrar actos violentos en nombre de una causa religiosa desvirtuada.

España no ha permanecido ajena a esta realidad. Según datos oficiales del Ministerio del Interior, desde 2013 hasta 2019 más de doscientos ciudadanos españoles se desplazaron como combatientes extranjeros hacia zonas de conflicto en Siria e Iraq, muchos provenientes de Ceuta, Melilla y áreas periféricas de grandes ciudades como Madrid, Barcelona o Valencia. Este fenómeno no solo implica riesgos durante su permanencia en dichas áreas, sino que se agudiza al retornar estos individuos con una formación militar específica, una narrativa radical reforzada y vínculos transnacionales activos, incrementando la amenaza terrorista interna. Este retorno constituye uno de los principales desafíos actuales para la seguridad española y europea, debido al complejo proceso probatorio necesario para imputar delitos cometidos en el extranjero y la dificultad para evaluar objetivamente su peligrosidad real en contextos urbanos donde suelen reintegrarse en entornos familiares o comunitarios.

La problemática del terrorismo yihadista se agrava por su capacidad adaptativa y descentralizada, funcionando mediante células autónomas, actores solitarios y redes informales. La internacionalización del conflicto tras las Primaveras Árabes ha facilitado el surgimiento de múltiples focos insurgentes en regiones como África del Norte, el Sahel o la Península Arábiga. Asimismo, la proclamación del Califato por Daesh no solo representó un intento de restauración política-religiosa sin precedentes desde la caída del Imperio Otomano, sino que también significó un cambio radical en la estrategia comunicativa del yihadismo,

utilizando herramientas digitales con fines propagandísticos y de reclutamiento global. La sofisticada narrativa mediática desplegada en revistas como Dabiq o Rumiya, sumada al uso intensivo de plataformas como Telegram o Twitter, ha consolidado al entorno virtual como el principal vector de radicalización.

En este contexto, España ha adoptado importantes reformas legislativas orientadas hacia una política criminal preventiva. La Ley Orgánica 13/2015 introdujo modificaciones sustanciales en los artículos 282 bis y 588 ter de la Ley de Enjuiciamiento Criminal, reconociendo jurídicamente la figura del Agente Encubierto Informático (AEI). Este agente especializado permite infiltrarse en redes digitales cerradas con identidad ficticia y recabar pruebas válidas en procesos judiciales, siempre bajo control judicial estricto y cumpliendo principios fundamentales como la legalidad, proporcionalidad y necesidad. Esta figura se ha convertido en esencial para la prevención efectiva, anticipando amenazas terroristas en fases iniciales y evitando su materialización violenta.

El análisis empírico realizado en esta tesis, basado en el estudio de múltiples operaciones policiales, jurisprudencia relevante y casos prácticos, evidencia el impacto significativo del Agente Encubierto Informático en la prevención y neutralización de amenazas yihadistas. Más del 90% de las detenciones por terrorismo en España desde 2015 están relacionadas con actividades en el ciberespacio (Ministerio del Interior, 2025). Casos como la Operación Silicon o la detención de células juveniles en Elche demuestran cómo la infiltración digital ha permitido desarticular grupos en fases tempranas, recabar pruebas concluyentes y prevenir atentados potenciales.

No obstante, la eficacia del Agente Encubierto Informático o Virtual no está exenta de dilemas éticos y jurídicos. Su empleo plantea debates sobre la privacidad, el equilibrio entre seguridad y libertad de expresión, así como la garantía plena de derechos fundamentales. Por ello, esta investigación propone la necesidad de mantener una supervisión judicial rigurosa, criterios claros de actuación y una delimitación precisa frente a figuras afines como el ciberpatrullero o el agente provocador, asegurando así su legitimidad constitucional.

Además, la radicalización yihadista continúa encontrando en jóvenes de segunda generación y conversos vulnerables un objetivo preferente. Factores como la frustración social, el desarraigo identitario y la narrativa épica promovida digitalmente siguen alimentando un reclutamiento preocupante. La figura del AEI

ha resultado particularmente efectiva en identificar estos procesos tempranos, permitiendo intervenciones preventivas antes de que se traduzcan en violencia efectiva.

La presente tesis doctoral plantea, por tanto, un modelo operativo y normativo integral que refuerza el papel del agente encubierto informático en el contexto español, sugiriendo mejoras en protocolos policiales, técnicas de infiltración y coordinación internacional. Se recomienda además potenciar programas de prevención comunitaria y educativa, adaptados a los nuevos entornos digitales, que complementen las intervenciones policiales.

Actualmente, en 2025, el terrorismo yihadista transita hacia una dinámica marcada por la descentralización y la instrumentalización estratégica de conflictos regionales para obtener impacto global. La actividad terrorista de organizaciones como el Estado Islámico del Khorasan (IS-K), que inicialmente operaba en Afganistán y Pakistán, se expande hacia Asia Central, Europa y África Occidental, aprovechando vacíos de seguridad, conflictos étnicos y fragilidades institucionales. Los recientes atentados en Moscú, Irán y Turquía reflejan claramente esta expansión y la nueva capacidad de acción global del IS-K. Por ello, se hace imprescindible enfocar los esfuerzos internacionales de contraterrorismo hacia estas regiones emergentes y entender las nuevas dinámicas locales y regionales como clave para prevenir futuras amenazas.

En conclusión, frente al carácter mutable, globalizado y digitalmente sofisticado del terrorismo yihadista, la figura del agente encubierto informático emerge como una herramienta crucial en la estrategia preventiva del Estado español. Su consolidación normativa, operacional y ética representa no solo una necesidad táctica inmediata, sino también una garantía esencial para mantener un equilibrio sostenible entre seguridad colectiva y libertades fundamentales, en un contexto marcado por la incertidumbre y la amenaza constante del terrorismo contemporáneo.

PALABRAS CLAVE

Terrorismo yihadista, Agente Encubierto Informático, radicalización, ciberterrorismo.

ABSTRACT

Nowadays, jihadist terrorism has emerged as one of the most significant global threats governments face, not only because of its devastating effects on public security but also due to its rapid expansion through the digital environment. Since the emergence in 2014 of the self-proclaimed Islamic Caliphate of Daesh in Syria and Iraq, cyberspace has become a privileged space for recruitment, indoctrination, financing, and dissemination of terrorist propaganda, leading to violent radicalization based on an extremist interpretation of Islam. Digital platforms such as social media, clandestine forums, and encrypted messaging channels have significantly enhanced sophisticated propaganda capable of deceiving thousands of followers willing to commit violent acts in the name of a distorted religious cause.

Spain has not remained immune to this reality. According to official data from the Spanish Ministry of the Interior, from 2013 to 2019, over two hundred Spanish citizens traveled as foreign fighters to conflict zones in Syria and Iraq, many from Ceuta, Melilla, and peripheral areas of large cities such as Madrid, Barcelona, or Valencia. This phenomenon involves risks not only during their stay in those conflict zones but also significantly increases upon their return, as these individuals possess specialized military training, reinforced radical narratives, and active transnational links, thus escalating the internal terrorist threat. This return poses one of the current primary challenges to Spanish and European security due to the complexity involved in judicially prosecuting crimes committed abroad and the difficulty in objectively assessing their real threat level within urban contexts, often reintegrated into family or community environments.

The jihadist terrorism problem worsens due to its adaptive and decentralized nature, operating through autonomous cells, lone actors, and informal networks. The internationalization of conflict following the Arab Spring facilitated multiple insurgent hotspots in regions such as North Africa, the Sahel, and the Arabian Peninsula. Furthermore, the proclamation of the Caliphate by Daesh represented not only an unprecedented attempt at political-religious restoration since the fall of the Ottoman Empire but also marked a radical shift in jihadist communication

strategies, using digital tools for global propaganda and recruitment purposes. The sophisticated media narrative deployed in magazines such as Dabiq or Rumiya, combined with intensive use of platforms like Telegram or Twitter, has established the virtual environment as the main vector for radicalization.

Within this context, Spain has undertaken significant legislative reforms geared towards a preventive criminal policy. Organic Law 13/2015 introduced substantial amendments to articles 282 bis and 588 ter j of the Spanish Criminal Procedure Act, legally recognizing the figure of the Undercover Cyber Agent (AEI). This specialized agent infiltrates closed digital networks with fictitious identities and collects legally valid evidence, always under strict judicial oversight and adhering to fundamental principles of legality, proportionality, and necessity. This figure has proven essential for effective prevention, anticipating terrorist threats in initial phases and preventing violent materialization.

The empirical analysis carried out in this thesis, based on numerous police operations, relevant jurisprudence, and practical case studies, demonstrates the significant impact of the Undercover Cyber Agent in preventing and neutralizing jihadist threats. Over 90% of terrorism-related arrests in Spain since 2015 have involved cyberspace activities (Ministry of Interior, 2025). Operations such as Silicon or the detention of youth cells in Elche illustrate how digital infiltration has allowed early disruption of terrorist groups, collection of conclusive evidence, and prevention of potential attacks.

However, the effectiveness of AEI is not without ethical and legal dilemmas. Its use raises debates regarding privacy, the balance between security and freedom of expression, and comprehensive protection of fundamental rights. Consequently, this research emphasizes the necessity of rigorous judicial supervision, clear action criteria, and precise delimitation from similar roles like cyber patrols or agent provocateurs, thereby ensuring constitutional legitimacy.

Furthermore, jihadist radicalization continues targeting vulnerable second-generation youths and converts. Factors such as social frustration, identity uprooting, and digitally promoted epic narratives continue fueling concerning recruitment. The AEI has proven particularly effective in identifying these early processes, facilitating preventive interventions before turning into effective violence.

Thus, this doctoral thesis proposes an operational and normative framework reinforcing the role of the Undercover Cyber Agent in the Spanish context, suggesting improvements in police protocols, infiltration techniques, and international coordination. Additionally, it recommends enhancing community-based and educational prevention programs adapted to new digital environments to complement police interventions.

Currently, in 2025, jihadist terrorism transitions towards dynamics marked by decentralization and strategic instrumentalization of regional conflicts to achieve global impact. Terrorist activities by organizations such as the Islamic State of Khorasan (IS-K), initially operating in Afghanistan and Pakistan, have expanded into Central Asia, Europe, and West Africa, exploiting security vacuums, ethnic conflicts, and institutional fragilities. Recent attacks in Moscow, Iran, and Turkey clearly illustrate this global expansion and IS-K's enhanced global operational capability. Therefore, international counterterrorism efforts must prioritize emerging regions and comprehend these new local and regional dynamics to effectively prevent future threats.

In conclusion, given the mutable, globalized, and digitally sophisticated nature of jihadist terrorism, the Undercover Cyber Agent emerges as a critical tool in Spain's preventive strategy. Its normative, operational, and ethical consolidation represents not only an immediate tactical necessity but also an essential guarantee to maintain a sustainable balance between collective security and fundamental freedoms, in a context characterized by uncertainty and constant threat from contemporary terrorism.

PALABRAS CLAVE

Jihadist terrorism, Undercover Cyber Agent, radicalization, cyber-terrorism.

AGRADECIMIENTOS

“El Guardia Civil no debe ser temido sino de los malhechores, ni temible sino a los enemigos del orden. Procurará ser siempre un pronóstico feliz para el afligido, y que a su presentación el que se creía cercado de asesinos, se vea libre de ellos; el que tenía su casa presa de las llamas, considere el incendio apagado; el que veía a su hijo arrastrado por la corriente de las aguas, lo crea salvado...”

Estas palabras, grabadas en la conciencia de quien ha jurado servir con honor a su Patria, resumen el espíritu de una vida entregada al deber y al bien común. Pero ningún camino, por exigente que sea, se transita solo. Este trabajo es fruto de muchas manos invisibles y de muchos corazones que, aun en la distancia, nunca dejaron de creer y acompañarme.

Mi primer y más profundo agradecimiento es para mis padres, pilares de mi vida y forjadores de mi carácter. A vosotros debo no solo los valores que me sostienen, sino también el ejemplo de una familia unida, generosa y firme, que hoy intento honrar y reproducir como modelo en mi propio hogar.

A mi familia, mi gratitud más íntima. Vuestra paciencia, vuestra ternura, vuestra fortaleza en los silencios y en las ausencias —tan frecuentes como injustas— han sido la brújula que ha guiado este trayecto. Nunca podré devolveros todo el cariño que os correspondía y que tantas veces dejé en pausa por cumplir este objetivo.

A mis hermanas, gracias por estar siempre, incluso en los días donde la sombra parecía más larga que la luz. Vuestra voz, vuestra fe y vuestro abrazo oportuno han sido el recordatorio constante de que la familia es la trinchera más noble en cualquier combate, incluso en los del alma.

Agradezco con especial afecto a la Universidad Católica San Antonio de Murcia (UCAM), que ha sido mi casa durante toda mi etapa académica. Gracias por acogerme con generosidad y por ofrecerme un espacio de crecimiento personal y profesional. A mi Director de tesis, el Dr. D. César Augusto Giner Alegría, por creer en mí desde el primer momento, por su guía paciente, por sus palabras de ánimo en los momentos más inciertos, y, sobre todo, por el privilegio de poder contar con su amistad.

A la Guardia Civil, y en particular, a la Jefatura de Información y al Grupo de Información de la 5ª Zona de Murcia, unidades que me han forjado como hombre y como persona, me honro en haber servido en una de las estructuras más discretas pero decisivas del Estado. Haber formado parte de operaciones que otros solo podrán imaginar o leer en relatos de ficción es un privilegio reservado a quienes han conocido el sacrificio en silencio y la vocación sin aspavientos.

A mi compañero y guía, D. José Antonio Rodríguez Puertas, porque sin tu apoyo constante, tu ejemplo profesional y tu confianza en mí, jamás me habría convertido en el profesional que soy hoy. Fuiste el arquitecto silencioso de mi vocación, el que supo despertar en mí esa mirada que escudriña lo invisible y convertir una intuición dispersa en una herramienta afinada y certera. Gracias por moldearme con exigencia, por sostenerme con lealtad y por creer en mí incluso cuando yo dudaba. Si hoy soy el analista que soñaba ser, es porque tú estuviste allí, forjando con paciencia lo que otros solo ven ya terminado.

Y a mis amigos, José Ángel, Rojo, Juanma, Javi, Chema y Fran, gracias por saber estar sin condiciones, por acompañar en los silencios y por sostener sin pedir nada a cambio. Vuestra lealtad discreta y constante ha sido refugio en los días más largos y faro en los momentos de duda.

A todos vosotros, de corazón, gracias.

Andrés Soriano.

“El Guardia Civil no busca la gloria, sino la protección del
inocente, aun cuando su rostro quede oculto y su nombre jamás
pronunciado.”

— Inspirado en la Cartilla del Guardia Civil.
(Duque de Ahumada, 1845)

ÍNDICE GENERAL

RESUMEN	7
I - INTRODUCCIÓN	29
II - OBJETIVOS	37
2.1. Objetivos Generales.....	¡Error! Marcador no definido.
2.2. Objetivos específicos	¡Error! Marcador no definido.
III - METODOLOGÍA	41
IV - EL TERRORISMO YIHADISTA COMO FENÓMENO GLOBAL	47
5.1. Conceptualización del terrorismo yihadista.....	47
5.2. Características distintivas del terrorismo yihadista respecto a otras formas de terrorismo	49
5.3. Reconfiguración e internacionalización del yihadismo	53
5.4. España en el radar del yihadismo global	56
V - LA REVELACIÓN ISLÁMICA FRENTE AL ISLAMISMO POLÍTICO TRANSNACIONAL	63
5.1. El islam como último eslabón de la cadena profética.....	63
5.2. Movimientos islamistas transnacionales: tradición, política y religión.	67
5.2.1. Los Hermanos Musulmanes.....	67
5.2.2. El Hizb Ut-Tahrir Al-Islami (HuT).....	73
VI - CORÁN Y ESPADA: LA APROPIACIÓN YIHADISTA DEL MENSAJE DIVINO	83
6.1. LA YIHAD: DE MANDATO ESPIRITUAL A ESTRATEGIA TERRORISTA.....	83

6.2.	LA EXEGESIS VIOLENTA DEL CORÁN Y SU LEGITIMACIÓN PARA EL COMBATE	85
6.3.	DE AL-QAEDA A DAESH Y SU COSMOVISIÓN DE LA YIHAD COMO FORMA DE GUERRA GLOBAL	91
6.4.	DEL FRENTE DE BATALLA AL CIBERESPACIO: LA YIHAD COMO INSURRECCIÓN DIGITAL DESCENTRALIZADA.....	93
VII -	uso del entorno digital por parte de al-qaeda y el estado islámico	99
7.1.	Formas de reclutamiento y adoctrinamiento a través de plataformas digitales	99
7.2.	Evolución en la financiación del terrorismo yihadista.....	107
7.2.1.	Mecanismos tradicionales de financiación.....	107
7.2.2.	Financiación del terrorismo a través de medios digitales.....	109
VIII -	ESTRATEGIAS DE COMUNICACIÓN DIGITAL, SEGMENTACIÓN IDEOLÓGICA Y CONSTRUCCIÓN DE LA MARCA YIHADISTA	117
8.1.	MARKETING Y TERRORISMO: CONVERGENCIA DE IDEOLOGÍAS.....	117
8.2.	SEGMENTACIÓN DEL PÚBLICO OBJETIVO YIHADISTA Y CONFIGURACIÓN DE MARCA	118
8.3.	NARRATIVA TRANSMEDIA Y ESTRATEGIA PROPAGANDÍSTICA	126
8.3.1.	Convergencia de formatos en la dimensión multimedia del relato yihadista	126
8.3.2.	De la doctrina al espectáculo propagandístico en el relato transmedia	128
8.3.3.	Las fábricas del relato: Al Hayat, Al Furqan, Al Amaq y las Willayat mediáticas del Califato	130
8.3.4.	Las revistas y su modulación ideológica del mensaje yihadista.....	132
8.3.5.	Análisis crítico del impacto de la propaganda yihadista.....	134
8.3.6.	La herencia del relato tras la caída del Califato islámico de Daesh.....	136

8.3.7.	La adopción del modelo comunicativo yihadista por otras organizaciones insurgentes.....	140
IX -	LA RADICALIZACIÓN YIHADISTA: TEORÍAS, PROCESOS Y PERFILES DE LOS INDIVIDUOS	144
9.1.	El Fenómeno de la radicalización yihadista en Europa y España.....	144
9.2.	Modelos Explicativos de la Radicalización Yihadista	148
9.3.	Factores psicosociales, identitarios y contextuales en la radicalización yihadista	152
9.4.	El papel del espacio digital en la radicalización, captación y adoctrinamiento del individuo.....	154
9.5.	Revisión Crítica sobre los programas de prevención y desradicalización.....	156
X -	La Figura del agente encubierto en el ordenamiento jurídico español	161
10.1.	Evolución legislativa y contexto normativo.....	161
10.1.1.	El Convenio de Budapest y la cooperación internacional en ciberdelincuencia.....	161
10.1.2.	Reformas clave del ordenamiento jurídico español: Ley Orgánica 5/2010, Ley Orgánica 2/2015 y Ley Orgánica 13/2015	163
10.2.	El Agente Encubierto tradicional.....	172
10.2.1.	Raíces históricas y práctica de la investigación encubierta en el ordenamiento jurídico español.....	172
10.2.2.	El Agente Encubierto tras la promulgación de la Ley de Enjuiciamiento Criminal de 1999.....	175
10.3.	Cuerpos policiales facultados para erigirse como Agente Encubierto	184
10.3.1.	La Policía autonómica catalana, los Mossos d'Esquadra como Policía Judicial	189
10.3.2.	La Policía autonómica vasca, la Ertzaintza como Policía Judicial	191

10.3.3.	La Policía Foral de Navarra como Policía Judicial	193
10.3.4.	El Servicio de Vigilancia Aduanera como Policía Judicial.....	195
XI -	EL AGENTE ENCUBIERTO INFORMÁTICO	199
11.1.	Evolución del paradigma criminal en la era digital	199
11.2.	El Agente Encubierto Informático	209
11.3.	Requisitos policiales y operativos del Agente Encubierto Informático 216	
XII -	EL AGENTE ENCUBIERTO INFORMÁTICO COMO HERRAMIENTA DE PREVENCIÓN DEL TERRORISMO YIHADISTA.....	222
12.1.	Dinámicas de radicalización online en España antes de la l.o 13/2015 222	
12.2.	Jurisprudencia y eficacia operativa del Agente Encubierto Informático en la lucha contra el Terrorismo Yihadista.....	227
12.2.1.	Diligencias Previas 27/2016 del Juzgado Central de Instrucción número 2 de la Audiencia Nacional, SAN 5286/2019, SAN 2203/2020 y STS 3448/2020: Operación Trankilo.	227
12.2.2.	Sumario 8/2016, SAN 3462/2018, STS 750/2019 y ATS 5261/2019: Operación Vértice.....	230
12.2.3.	SAN 3070/2019 y STS 3249/2021	236
12.2.4.	SAN 5421/2018 y SAN 1447/2019. Operación Silicon	242
12.2.5.	SAN 3054/2018 y STS 934/2019. Operación Talibán.....	248
XIII -	CONCLUSIONES.....	258
XIV -	REFERENCIAS BIBLIOGRÁFICAS	263
14.1.	BIBLIOGRAFÍA	263

SIGLAS Y ABREVIATURAS

AEI, Agente Encubierto Informático.

AEV, Agente Encubierto Virtual.

AQIS, Al-Qaeda en el Subcontinente Indio.

AQMI, Al-Qaeda en el Magreb Islámico.

AQPA, Al-Qaeda en la Península Arábiga.

BOE, Boletín Oficial del Estado.

CE, Constitución Española.

CENDOJ, Centro de Documentación Judicial.

CGPJ, Consejo General del Poder Judicial.

CITCO, Centro de Inteligencia contra el Terrorismo y el Crimen Organizado.

CNI, Centro Nacional de Inteligencia.

CP, Código Penal

CTED, Comité contra el Terrorismo del Consejo de Seguridad de la ONU,

DAESH, Estado Islámico de Irak y Siria.

EEUU, Estados Unidos de América.

ETA, Euskadi Ta Askatasuna

FARC, Fuerzas Armadas Revolucionarias de Colombia

FATF, Financial Action Task Force.

FCSE, Fuerzas y Cuerpos de Seguridad del Estado.

FJ, Fundamento Jurídico.

GIA, Grupo Islámico Armado.

GRAPO, Grupos de Resistencia Antifascista Primero de Octubre.

GSPC, Grupo Salafista para la Predicación y el Combate.

HHMM, Hermanos Musulmanes.

HUMINT, Human Intelligence.

ICCT, International Centre for Counterterrorism

ICSR, International Centre for the Study of Radicalization.

ISIS, Estado Islámico de Irak y Siria.

JSTOR, Journal Storage.

MPAIAC, Movimiento por la Autodeterminación e Independencia del Archipiélago Canario.

ONU, Organización de las Naciones Unidas.

OPSEC, Operational Security.

OSINT, Open Source Intelligence.

OTAN, Organización del Tratado del Atlántico Norte.

SOCMINT, Social Media Intelligence.

STC, Sentencia del Tribunal Constitucional.

STS, Sentencia del Tribunal Supremo.

TC, Tribunal Constitucional.

TEDH, Tribunal Europeo de Derechos Humanos.

TS, Tribunal Supremo.

UE, Unión Europea.

UNODC, United Nations Office on Drugs and Crime.

VPN, Virtual Private Network

I – INTRODUCCIÓN

I - INTRODUCCIÓN

Abordar la problemática contemporánea del terrorismo yihadista exige comprender que ya no nos enfrentamos a estructuras insurgentes convencionales, sino a un fenómeno mutante, híbrido y transnacional. Las organizaciones yihadistas han sabido adaptarse a las dinámicas de la globalización y de la revolución digital, reconfigurándose como redes descentralizadas, con capacidad para operar mediante células autónomas, lobos solitarios o combatientes retornados (Torres, 2020). Esta transición ha vaciado de sentido la noción clásica de “grupo terrorista” como entidad jerárquica y territorialmente anclada, dando paso a una amenaza líquida, invisible e inestable, cuyo campo de batalla se encuentra tanto en Siria, Iraq o cualquier zona de conflicto como en nuestros barrios, y cuyos combatientes a diferencia de sus antecesores pueden instruirse desde su propio ordenador sin necesidad de desplazarse a un campamento de entrenamiento en una zona controlada por la insurgencia.

La Comunidad Internacional tiene un gran reto que hacer frente, lograr frenar la propagación del terrorismo yihadista, una tipología de terrorismo que ha demostrado su resiliencia, capacidad destructiva y estrategia mediática con la que sembrar el terror e imponer su particular versión totalitaria del islam.

Ejemplo de ello, son los atentados del 11 de septiembre de 2001 en Nueva York y Washington (EEUU), el 11 de marzo de 2004 en los trenes con destino a la estación de Atocha en Madrid (España), el 7 de julio de 2005 en Londres (Reino Unido), el 13 de noviembre de 2015 en la sala Bataclán y el Estadio nacional en la ciudad de París (Francia), el 22 de marzo de 2016 en el aeropuerto de Bruselas (Bélgica), el 14 de julio de ese mismo año en Niza (Francia), el 17 de agosto de 2017 en Cataluña (España), entre otros muchos, hasta llegar a la última masacre cometida el 1 de enero del 2025 en Nueva Orleans (EEUU). La magnitud de estos atentados confirmó que el terrorismo yihadista había superado su estadio insurgente para transformarse en un fenómeno de alcance global, dotado de estructuras adaptativas, financiado por redes informales y con capacidad para influir en la agenda política y securitaria de las democracias occidentales (Reinares, 2015). Desde entonces, la amenaza dejó de percibirse como remota para instalarse como un factor estructural de inestabilidad.

El estallido de las llamadas “primaveras árabes” a partir de 2011, lejos de consolidar una transición democrática en el mundo musulmán, desencadenó un proceso de descomposición institucional que fue aprovechado por las corrientes salafistas más radicales. En países como Siria, Irak, Libia o Yemen, el colapso del Estado de derecho propició la emergencia de milicias islamistas, muchas de las cuales se integraron o juraron lealtad a Al Qaeda y posteriormente a Daesh (Gerges, 2016).

El vacío de poder y la proliferación de armas crearon las condiciones idóneas para el auge del terrorismo de inspiración yihadista. El conflicto sirio-iraquí se convirtió en el epicentro de la yihad global, atrayendo a más de 40.000 combatientes extranjeros, entre ellos más de 5.000 europeos (Soufan Group, 2015). España no fue ajena a esta dinámica: entre 2013 y 2019 se contabilizaron más de doscientos desplazamientos de foreign fighters hacia zonas de conflicto, muchos de ellos procedentes de Ceuta, Melilla o barrios periféricos de grandes ciudades como Barcelona, Madrid o Valencia (Ministerio del Interior, 2022). La narrativa de la umma en decadencia y humillada por occidente, el martirio glorioso y el paraíso ganado mediante la yihad en el camino de Allah caló especialmente entre jóvenes con pocas aspiraciones de futuro o en procesos de búsqueda identitaria.

La dimensión internacional del conflicto agravó el problema de seguridad, pues estos “foreign fighters” no solo combatieron, sino que regresaron a sus países de origen con entrenamiento, vínculos transnacionales y una narrativa legitimadora del martirio y la violencia como forma de redención.

La proclamación del Califato Islámico por parte de Daesh en junio de 2014, representó la culminación de esta deriva. Por primera vez desde la caída del Imperio Otomano, un grupo yihadista reclamaba no solo territorio, sino soberanía política y religiosa. Daesh, a diferencia de Al Qaeda, priorizó el control territorial, la expansión militar y la gestión de la vida cotidiana conforme a los preceptos más rigoristas del salafismo yihadista. Pero su mayor innovación fue comunicacional, pues convirtieron la propaganda en arma de guerra, el martirio en estética viral, y el terror en narrativa globalizada (Torres, 2016).

Revistas como Dabiq o Rumiya, vídeos editados con calidad cinematográfica y la difusión masiva de contenidos violentos en redes sociales como Telegram o X (Twitter), hicieron del ciberespacio un nuevo frente de batalla. Esta capacidad de producir y exportar ideología radicalizada convirtió a Daesh en

un fenómeno sin precedentes, capaz de movilizar a individuos aislados o células dormidas en cualquier punto del planeta, incluida España.

La irrupción de estas nuevas formas de terrorismo digital y descentralizado obligó al legislador español a reformular las herramientas de investigación penal. Hasta 2015, la Ley de Enjuiciamiento Criminal apenas contemplaba la posibilidad de actuación encubierta en el ciberespacio. Sin embargo, ante la creciente sofisticación de los métodos de radicalización online, y tras diversas operaciones frustradas por falta de cobertura legal, se aprobó la Ley Orgánica 13/2015, que reformó los artículos 282 bis y 282 ter de la LECrim, dotando de encaje jurídico al agente encubierto informático (AEI) como figura específica de investigación policial.

Esta figura no solo permite a las Fuerzas y Cuerpos de Seguridad infiltrarse en redes digitales cerradas con una identidad ficticia, sino que posibilita la recolección de pruebas en entornos virtuales con plena validez procesal, siempre bajo control judicial y respetando los principios de legalidad, necesidad y proporcionalidad.

Con la derrota territorial del Daesh en 2019, se abrió una nueva fase del terrorismo yihadista caracterizada por la dispersión de sus cuadros, el retorno de combatientes a Europa, y la radicalización de nuevas generaciones nacidas en el seno de familias yihadistas. España, aunque no ha sido uno de los países con más yihadistas desplazados, sí ha registrado más de un centenar de retornados (Reinares y García-Calvo, 2023), muchos de los cuales regresan con entrenamiento, motivación ideológica reforzada y voluntad de continuar la yihad desde suelo europeo.

En paralelo, los hijos de combatientes o de individuos radicalizados, criados en contextos culturales de odio hacia Occidente, representan un nuevo desafío para la prevención. Estas segundas generaciones, sometidas a procesos de socialización dual y desarraigo identitario, encuentran en la narrativa yihadista un marco de sentido y pertenencia, consolidando al espacio virtual como el principal vector de captación y adoctrinamiento. Del mismo modo, el proyecto de reconquista y radicalización sobre Al-Andalus, tal y como ha sido abordado por el profesor Torres (2014), demuestra cómo la narrativa digital centrada en la "recuperación de tierras perdidas", especialmente en alusión a la antigua presencia musulmana en

España, continúa alimentando discursos de odio entre jóvenes musulmanes de segunda generación.

Las tecnologías de la información han alterado profundamente el modo de operar del yihadismo. Los foros clandestinos, las plataformas de mensajería cifradas, las redes sociales y los videojuegos online han sido instrumentalizados como espacios de socialización radical, planificación de atentados y difusión de propaganda de adoctrinamiento ideológico y militar (Europol, 2022). La inmaterialidad del entorno digital dificulta la detección de amenazas, desborda las técnicas tradicionales de vigilancia y exige una actualización constante de los instrumentos legales y operativos.

En este contexto, el AEI emerge como uno de los pocos recursos capaces de introducirse en dichos entornos con el sigilo y la flexibilidad necesarias. Su intervención ha sido decisiva en la neutralización de múltiples células en España, como demuestran los datos del Ministerio del Interior: más del 90 % de las detenciones por terrorismo yihadista desde 2015 han estado vinculadas a actuaciones en el ciberespacio (Ministerio del Interior, 2025). Por ello, la figura del agente encubierto informático no solo representa una herramienta de investigación, sino una estrategia de anticipación frente a amenazas difusas. Permite detectar discursos incipientes de odio, identificar nodos de reclutamiento y desmontar redes antes de que se traduzcan en acciones violentas o atentados terroristas. Aporta pruebas válidas que refuerzan la respuesta penal y, en muchos casos, contribuye a la disuasión del delito mediante la percepción de vigilancia.

Como señala el magistrado Javier Gómez Bermúdez (2021), “la eficacia del agente encubierto digital reside en su capacidad para iluminar los rincones oscuros de Internet donde germina la violencia”. Su papel no es invasivo, sino quirúrgico; no sustituye al debido proceso, sino que lo fortalece, ofreciendo a los jueces una vía legal para actuar con prontitud frente a conductas incipientes.

Por todo ello, la presente tesis se plantea como objetivo analizar en profundidad la figura del agente encubierto informático en el marco jurídico y criminológico español, su evolución, sus fundamentos normativos y su impacto real en la prevención del terrorismo yihadista. Para ello, se parte de una revisión doctrinal, legislativa y jurisprudencial, complementada con el estudio de casos, operaciones policiales y datos oficiales que nos permitirán dilucidar la efectividad de dicha medida investigativa.

Desde una perspectiva práctica, la tesis intentará brindar herramientas para el diseño de protocolos policiales y técnicas de infiltración en dichos entornos, aplicables tanto a la prevención como a la judicialización de los delitos de terrorismo en su fase embrionaria.

A lo largo de los capítulos que siguen se abordará, primero, el contexto ideológico y estratégico del yihadismo contemporáneo, desde sus raíces doctrinales hasta su proyección digital. Posteriormente, se examinará la regulación legal del AEI, sus límites constitucionales y los dilemas que plantea en relación con derechos fundamentales. Finalmente, se evaluará su eficacia operativa y se propondrán recomendaciones para su consolidación como figura central en la lucha contra la amenaza del terrorismo yihadista global.

II – OBJETIVOS

II - OBJETIVOS

El objetivo general del presente estudio consiste en examinar, desde una perspectiva multidisciplinar, jurídica, criminológica y operativa, la figura del Agente Encubierto Informático en el marco de la lucha contra el terrorismo yihadista en España, evaluando su eficacia preventiva en entornos digitales, su encaje normativo en el ordenamiento jurídico español, sus límites constitucionales y su capacidad para anticipar, detectar y neutralizar amenazas yihadistas incipientes en la red.

Como objetivos específicos se encuentran los siguientes:

1. Establecer un análisis histórico, doctrinal y estructural del yihadismo contemporáneo.
2. Estudiar las estrategias digitales del terrorismo yihadista: propaganda, captación, radicalización, adoctrinamiento técnico y táctico, y financiación en los entornos virtuales.
3. Delimitar la arquitectura funcional del ecosistema digital yihadista: organización, segmentación y dinámicas de interacción en el ciberespacio.
4. Analizar operativa y jurisprudencialmente casos reales de sentencias en las que el Agente Encubierto Informático haya participado para la desarticulación de la célula terrorista.
5. Construir un marco teórico multidisciplinar sobre los procesos de radicalización islamistas.
6. Examinar la evolución normativa y jurisprudencial que regula la figura del Agente Encubierto Informático en el ordenamiento jurídico español.
7. Comparar la figura del Agente Encubierto Informático frente a otras figuras afines al proceso penal.

8. Estudiar cualitativamente operaciones policiales con Agentes Encubiertos Informáticos y analizar su eficacia operativa, validez probatoria y límites éticos.

III - METODOLOGÍA

III - METODOLOGÍA

La presente investigación adopta un enfoque metodológico de carácter cualitativo y multidisciplinar, orientado al análisis crítico, interpretativo y propositivo de la figura del agente encubierto informático (AEI) en el marco de la prevención del terrorismo yihadista. Debido a la complejidad del objeto de estudio, que integra elementos jurídicos, criminológicos, operativos, tecnológicos y doctrinales, se ha recurrido a un modelo metodológico mixto, predominantemente cualitativo, basado en el análisis documental, normativo, jurisprudencial y comparado, complementado con un enfoque inductivo que permita formular propuestas de actuación concretas.

La investigación se estructura conforme a un diseño exploratorio y descriptivo, con fines explicativos y propositivos. Explora un campo doctrinal aun escasamente desarrollado en la literatura jurídica española y europea, como es la figura del AEI en operaciones antiterroristas, y describe su contexto normativo, sus fundamentos constitucionales, su uso en operaciones reales y sus potencialidades como herramienta de prevención en el ámbito de la seguridad nacional.

Para alcanzar los objetivos propuestos, se ha procedido a una revisión sistemática y selectiva de un amplio conjunto de fuentes primarias y secundarias, tanto nacionales como internacionales. Estas se clasifican del siguiente modo:

- **Fuentes normativas:** legislación española relevante (especialmente la Ley de Enjuiciamiento Criminal tras la reforma de la L.O. 13/2015, y sus artículos 282 bis y ter), normativa procesal, penal y constitucional, así como tratados internacionales y directivas europeas sobre cooperación antiterrorista, uso de técnicas especiales de investigación y derechos fundamentales.
- **Fuentes jurisprudenciales:** sentencias del Tribunal Supremo, la Audiencia Nacional, el Tribunal Constitucional y el Tribunal Europeo de Derechos Humanos, relativas a actuaciones encubiertas, protección del secreto de las comunicaciones, prueba ilícita, proporcionalidad, y derecho a un proceso con todas las garantías. Dada la escasez de resoluciones específicas sobre el

AEI, se ha ampliado el análisis a sentencias relativas a figuras afines (agentes encubiertos clásicos, provocadores, ciberpatrullaje).

- **Fuentes doctrinales:** se ha consultado una amplia variedad de libros, tesis doctorales, monografías jurídicas y criminológicas de alto impacto, artículos indexados en revistas especializadas (preferentemente Q1-Q2 en JCR o Scopus) y ensayos académicos en español, inglés, francés e italiano, que abordan desde distintas ópticas el fenómeno del terrorismo yihadista, la radicalización violenta, el derecho penal del enemigo, los métodos de inteligencia, la cibervigilancia y las técnicas de investigación encubierta.
- **Informes institucionales y bases empíricas:** se incluyen documentos oficiales del Ministerio del Interior, la Secretaría de Estado de Seguridad, la Fiscalía de la Audiencia Nacional, Europol, Eurojust, el Departamento de Seguridad Nacional y el Real Instituto Elcano. Estos informes han sido clave para contextualizar empíricamente el fenómeno de la radicalización yihadista, los perfiles de los retornados, el uso del entorno virtual y el impacto de operaciones reales de prevención.
- **Recursos académicos digitales:** se ha realizado una búsqueda exhaustiva en bases de datos académicas como Dialnet, Google Scholar, JSTOR, Scopus, SciELO, etc. priorizando fuentes posteriores al año 2015, a fin de asegurar la máxima actualidad y pertinencia de la literatura empleada. Solo en casos justificadamente históricos se han incluido referencias anteriores, por ejemplo, para explicar los orígenes del salafismo-yihadista, la evolución doctrinal de Al Qaeda o los antecedentes del agente encubierto físico.
- **Lenguas y procedencia de fuentes:** si bien el corpus principal está en español, se han incorporado textos en inglés, francés y árabe, dada la relevancia de la cooperación internacional en la lucha contra el terrorismo y la producción doctrinal en estos idiomas sobre la materia.

El procedimiento ha seguido varias fases complementarias:

- **Fase exploratoria:** identificación de las categorías de análisis clave (yihadismo digital, AEI, técnicas de infiltración, derechos fundamentales, procesos de radicalización, jurisprudencia relevante, operaciones policiales significativas).
- **Fase documental:** análisis y sistematización de contenidos extraídos de las fuentes antes mencionadas, organizando los datos por bloques temáticos, cronológicos y normativos.
- **Fase analítica:** interpretación crítica de los textos y casos seleccionados, estableciendo relaciones entre teoría y práctica, normas y operaciones, doctrina y realidad operativa. Se ha utilizado un enfoque hermenéutico y constructivista, donde el investigador analiza el significado jurídico, social y ético de las herramientas analizadas, y propone su reformulación.

El enfoque elegido se justifica por la propia naturaleza del objeto de estudio: el terrorismo yihadista es un fenómeno de alta complejidad, con múltiples dimensiones ideológicas, sociales, criminales y tecnológicas, que exige una mirada transversal. La figura del AEI, a su vez, se encuentra en la intersección entre la dogmática penal, el derecho procesal, el derecho constitucional, la criminología empírica y la ciencia de la seguridad, lo que obliga a adoptar un método integrador, reflexivo y contextualizado.

Asimismo, la elección de una metodología cualitativa responde a la imposibilidad de cuantificar exhaustivamente muchas de las variables implicadas (por razones de confidencialidad operativa, escasa jurisprudencia o dispersión doctrinal), pero también al deseo de profundizar en el análisis conceptual y propositivo de una figura relativamente reciente en nuestro ordenamiento, cuyo potencial preventivo está aún por desarrollar.

IV – EL TERRORISMO YIHADISTA COMO FENÓMENO GLOBAL

IV - EL TERRORISMO YIHADISTA COMO FENÓMENO GLOBAL

5.1. CONCEPTUALIZACIÓN DEL TERRORISMO YIHADISTA

La definición del terrorismo ha sido siempre una tarea particularmente compleja, dada su naturaleza dinámica, su instrumentalización política, y las profundas diferencias ideológicas entre los actores estatales e internacionales implicados. En efecto, como afirma Vacas (2011), cada Estado interpreta el terrorismo según su experiencia histórica, valores básicos asumidos y prioridades diplomáticas, lo que explica la falta de un consenso universalmente aceptado sobre qué constituye exactamente un acto terrorista (p. 24).

Desde una perspectiva académica, De la Corte (2006) aporta claridad al definir el terrorismo como: “una sucesión premeditada de actos violentos e intimidatorios dirigidos contra población no combatiente, diseñados para ejercer una presión psicológica que afecta a una audiencia considerablemente más amplia que sus víctimas directas, buscando alcanzar objetivos principalmente políticos” (p. 43). Esta definición se completa al considerar el componente psicológico como eje central en la estrategia terrorista moderna. No se trata solo de causar daño físico o material, sino de generar un miedo profundo y generalizado, una incertidumbre que fractura el tejido social y deslegitima a las autoridades políticas. Como señala Münkler (2005), “la violencia terrorista actual tiene un objetivo fundamentalmente psicológico, más allá del daño inmediato que pueda provocar” (p. 132).

En este sentido, la Organización del Tratado del Atlántico Norte (OTAN) adopta una definición muy próxima, enfatizando su naturaleza coercitiva mediante el “uso o amenaza ilegal de violencia contra individuos o propiedades, con el propósito de intimidar a gobiernos o sociedades para lograr fines políticos, religiosos o ideológicos específicos” (OTAN, 2016).

En la misma línea, el Departamento de Estado de EE. UU. enfatiza que la violencia terrorista es premeditada, políticamente motivada y dirigida principalmente hacia objetivos civiles, persiguiendo ejercer una influencia desproporcionada sobre audiencias amplias (U.S. Department of State, 2019). Esta perspectiva pone de relieve que el terrorismo es esencialmente comunicativo y

simbólico, valiéndose de los medios masivos y digitales para amplificar sus mensajes.

Contrariamente a ciertas percepciones mediáticas que presentan a los actos terroristas como irracionales o fruto exclusivo del fanatismo, Núñez (2015) advierte sobre el error estratégico de esta interpretación. Los actos terroristas generalmente responden a un cálculo racional y estratégico claro, por lo que ignorar esta realidad dificulta enormemente el diseño de políticas preventivas y represivas adecuadas. Rafael Calduch (2001) refuerza esta idea al sostener que el terrorismo no es simplemente violencia, sino una estrategia calculada cuyo objetivo último es alterar el equilibrio político vigente mediante el terror social (p. 14-15).

Sin embargo, también es preciso señalar que algunas manifestaciones terroristas han carecido de esta racionalidad instrumental, como por ejemplo los ataques apocalípticos perpetrados por la secta japonesa Aum Shinrikyo en 1995, cuyas motivaciones eran mesiánicas y no políticas en sentido estricto (Dershowitz, 2004). A pesar de estas excepciones, la mayoría de las acciones terroristas contemporáneas, y particularmente el terrorismo yihadista, reflejan una racionalidad calculada y estratégica, cuyo objetivo último es inducir cambios sociales y políticos significativos a través del terror.

En efecto, el terrorismo yihadista contemporáneo merece una consideración específica, pues fusiona de manera singular motivaciones políticas y religiosas. Este tipo de terrorismo, cuya expansión se intensificó notablemente tras los atentados del 11-S en Estados Unidos, encarna lo que Rapoport (2004) denomina la cuarta ola del terrorismo moderno: la ola religiosa, caracterizada por una visión apocalíptica, transnacional y moralmente absolutista, donde el uso de la violencia es presentado como un mandato divino contra los considerados “infieles” o “apóstatas”. Ranstorp (2004) precisa que la violencia yihadista interpreta su misión como una respuesta legítima y necesaria frente a la opresión percibida contra los musulmanes, justificando así ataques cada vez más letales y mediáticos (p. 204).

La Estrategia contra el Terrorismo de la Unión Europea (2005) identifica claramente al terrorismo yihadista como una amenaza existencial a los valores democráticos, las libertades fundamentales y la seguridad de sus ciudadanos, destacando especialmente grupos como Daesh y Al Qaeda como sus principales exponentes.

Teniendo en cuenta estas perspectivas y la riqueza de aportaciones académicas, jurídicas y gubernamentales se propone una definición propia integradora, que recoge las características esenciales del terrorismo contemporáneo con especial énfasis en la modalidad yihadista:

El terrorismo contemporáneo, particularmente el terrorismo yihadista, es una estrategia política que emplea de manera premeditada y sistemática la violencia extrema contra objetivos civiles e instituciones simbólicas, con el propósito de generar un profundo impacto psicológico y mediático que trasciende ampliamente el daño material inmediato. Esta modalidad específica del terrorismo justifica sus actos a través de una interpretación fundamentalista y violenta del islam, promoviendo una visión del mundo polarizada entre creyentes y no creyentes, legitimando así la violencia como un deber divino frente a supuestas agresiones externas contra el mundo musulmán. Su naturaleza híbrida integra tácticas convencionales e insurgentes, junto con una sofisticada utilización de tecnologías de la información y plataformas mediáticas para adoctrinar, reclutar y difundir globalmente su ideario radical, con el objetivo último de desestabilizar y modificar profundamente el orden político y social existente.

En definitiva, comprender adecuadamente la naturaleza racional y estratégica del terrorismo, especialmente en su variante yihadista, resulta indispensable para desarrollar estrategias de prevención y neutralización eficaces. Como bien concluye Reinares (2006), aunque reconocer la racionalidad del terrorismo no implica su legitimación ni justificación ética, sí resulta imprescindible para combatir eficazmente sus manifestaciones.

5.2. CARACTERÍSTICAS DISTINTIVAS DEL TERRORISMO YIHADISTA RESPECTO A OTRAS FORMAS DE TERRORISMO

El terrorismo yihadista, aunque comparte algunos rasgos comunes con otras modalidades terroristas, posee características distintivas que lo diferencian sustancialmente y le otorgan una especificidad propia. La primera de estas particularidades es la centralidad que adquiere la religión, específicamente una interpretación radicalizada y fundamentalista del islam bajo los postulados salafistas yihadistas, como justificación y motor ideológico de la violencia ejercida.

Este extremismo religioso está sustentado en la convicción profunda de librar una guerra legitimada como sagrada (yihad) contra todos aquellos que se consideran enemigos del islam auténtico, interpretado desde una perspectiva extremadamente literal y dogmática (Torres, 2007).

Una característica especialmente singular del terrorismo yihadista es su pretensión global, proyectándose más allá de los conflictos regionales o nacionales y defendiendo una lucha transnacional que no reconoce fronteras geográficas. A diferencia de organizaciones como ETA, el IRA o las FARC, cuya lucha se limitaba fundamentalmente a reivindicaciones territoriales específicas, grupos como Al Qaeda y Daesh sostienen una guerra global cuyo objetivo último es transformar el orden internacional desde una perspectiva religiosa fundamentalista (Rapoport, 2004).

En este contexto, resulta especialmente ilustrativa la tesis planteada por David Rapoport sobre las olas del terrorismo. Según Rapoport, el terrorismo yihadista representa la cuarta ola del terrorismo moderno, conocida como la "ola religiosa", caracterizada por una motivación principalmente espiritual, en contraste con las anteriores oleadas terroristas, anarquista, nacionalista y marxista. El terrorismo religioso, del cual el yihadismo es su manifestación más potente y contemporánea, se distingue por la absoluta convicción moral y religiosa de sus combatientes, dispuestos a sacrificarse sin límites en busca de la recompensa divina prometida tras la muerte (Rapoport, 2004) y su ascensión al Paraíso como "mártir en el camino de Allah".

En consonancia con esto, una de las prácticas distintivas del terrorismo yihadista es el empleo sistemático del martirio y las operaciones suicidas como técnica operativa habitual. La figura del mártir o *shahid* adquiere una importancia central en la narrativa yihadista, elevando a quienes sacrifican su vida en combate a un nivel casi sagrado, convirtiendo así la violencia suicida en una herramienta fundamental de reclutamiento y propaganda. Esta estrategia, cuya finalidad última es generar una fuerte impresión psicológica tanto en los enemigos directos como en la audiencia internacional, encuentra una justificación teológica específica dentro del discurso salafista-yihadista, lo que la convierte en una táctica particularmente eficaz y letal (Reinares, 2006).

Otra característica crucial del terrorismo yihadista contemporáneo es su altísima capacidad adaptativa y el uso extensivo de medios digitales y redes

sociales. Las plataformas digitales son utilizadas no solo para la difusión de propaganda, sino también para el reclutamiento, la financiación clandestina, la radicalización, el adoctrinamiento en tácticas, técnicas y procedimientos militares y de combate sin la necesidad de desplazarse a los campos de entrenamiento situados en zona de conflicto y la coordinación operativa internacional de sus células durmientes e integrantes. Como señala Torres (2013), "el terrorismo yihadista ha encontrado en internet un instrumento perfecto para proyectar su narrativa ideológica radicalizada, movilizando adeptos en contextos muy diversos sin necesidad de contacto físico o presencial" (p. 3).

Asimismo, el terrorismo yihadista se caracteriza por una estructura organizativa descentralizada y fluida, que combina jerarquías tradicionales con células autónomas o lobos solitarios que operan con escaso o ningún contacto directo con los líderes centrales. Esta descentralización operativa ha supuesto un desafío significativo para las fuerzas de seguridad internacionales, dificultando enormemente las tareas de detección, infiltración y prevención de ataques terroristas. Además, su capacidad para regenerarse tras sufrir golpes significativos en su liderazgo muestra una resiliencia organizacional que incrementa su peligrosidad y prolonga su existencia en el tiempo (Alonso, 2015).

Junto a esto, el terrorismo yihadista destaca también por su instrumentalización deliberada y estratégica del simbolismo mediático. Los atentados del 11 de septiembre en Estados Unidos, los ataques en París (2015), Bruselas (2016) o Barcelona (2017), fueron diseñados específicamente para generar un máximo impacto simbólico y psicológico, apuntando contra iconos representativos del estilo de vida occidental para maximizar el alcance mediático y difundir globalmente su mensaje extremista. Ranstorp (2004) subraya cómo la capacidad del terrorismo yihadista para seleccionar objetivos altamente simbólicos es una de las razones fundamentales de su eficacia comunicativa global, consiguiendo propagar el terror más allá de las fronteras físicas inmediatas del atentado.

Finalmente, es imprescindible mencionar el objetivo último y radical del terrorismo yihadista: la restauración del califato islámico como sistema político y religioso supremo sobre la umma global, un objetivo explícitamente defendido por Daesh desde su irrupción en Siria e Irak en 2014. A diferencia de otras modalidades terroristas, cuya agenda política puede tener reivindicaciones más limitadas y

negociables, la aspiración de crear un orden político-religioso universal regido por la Sharía o ley islámica no admite compromisos o negociaciones intermedias. Esto explica la extrema radicalidad y persistencia con la que estas organizaciones combaten y propagan su mensaje extremista, sin intención alguna de coexistencia pacífica con sistemas políticos y culturales distintos a los dictados por su ideología totalitaria (Jordán, 2010).

Por todo ello, la comprensión profunda de estas características específicas del terrorismo yihadista contemporáneo resulta indispensable para desarrollar estrategias eficaces de prevención, lucha y desradicalización a nivel global, enfrentando así una amenaza compleja que continúa evolucionando y adaptándose de manera sobresaliente en el tiempo.

Ante este nuevo escenario, el ordenamiento jurídico español ha debido transformarse profundamente. El modelo legislativo concebido para combatir a ETA y GRAPO principalmente, centrado en el castigo del hecho terrorista consumado o de sus actos preparatorios inmediatos, resultaba insuficiente frente a un terrorismo que se gestaba en la sombra, en foros digitales, mediante adoctrinamiento, autoformación y vínculos difusos. Sin embargo, el gran punto de inflexión se produce tras los atentados del 11-M de 2004 en Madrid. A partir de ese momento, comienza una reforma penal progresiva cuyo eje es la anticipación penal, orientada a neutralizar la amenaza antes de que se materialice. Esta lógica se concreta en varias modificaciones del Código Penal español:

- Ley Orgánica 5/2010: introduce el artículo 577 bis, que tipifica la formación pasiva y activa para actividades terroristas como la captación y el adoctrinamiento.
- Ley Orgánica 2/2015, que reforma los artículos 571 a 580, incorporando delitos como el autoadoctrinamiento y la captación en línea
- Se amplía el concepto de terrorismo para incluir no solo a quienes ejecutan atentados, sino también a quienes “difunden ideas que promuevan el uso de la violencia con fines subversivos del orden constitucional” (art. 578 CP).

En palabras de Reinares (2021), se trata de una “política criminal de la prevención reforzada”, que desplaza el foco desde el atentado hacia el ecosistema ideológico que lo posibilita. En este marco, la figura del agente encubierto informático (regulada en los artículos 282 bis y 588 ter j de la Ley de Enjuiciamiento

Criminal) se convierte en pieza clave para investigar las redes invisibles de radicalización y aportar pruebas válidas en procesos judiciales.

Si bien, este nuevo paradigma no está exento de desafíos, pues como advierte Camino (2022) tensiona el principio de mínima intervención penal, plantea dilemas sobre la libertad de expresión religiosa y exige un equilibrio constante entre seguridad y garantías procesales. Sin embargo, como demuestra la jurisprudencia y las numerosas operaciones policiales realizadas en los últimos años, estas reformas han sido esenciales para evitar la comisión de atentados terroristas y la desarticulación de células operativas y actores solitarios determinados a ejercer la violencia.

5.3. RECONFIGURACIÓN E INTERNACIONALIZACIÓN DEL YIHADISMO

La irrupción del terrorismo yihadista en la agenda internacional tras los atentados del 11 de septiembre de 2001 en Estados Unidos marcó el inicio de una nueva fase en la proyección global de la yihad armada. La guerra contra el terrorismo iniciada por Washington, con las invasiones de Afganistán e Irak como ejes fundamentales, no solo no logró contener el fenómeno, sino que contribuyó a su expansión, dando lugar a un nuevo mapa de conflictos que actuó como polo de atracción para miles de combatientes extranjeros (Neumann, 2016).

A diferencia de los conflictos islamistas anteriores, como la guerra de Afganistán en los años ochenta, donde los muyahidines combatían a una potencia ocupante, Rusia, con el respaldo de Occidente; la etapa posterior a 2001 se caracterizó por una fragmentación del frente yihadista. A partir de entonces, surgieron múltiples focos de insurgencia con dinámicas propias: desde Al Qaeda en la Península Arábiga (AQPA) hasta el surgimiento de Al Shabaab en Somalia, pasando por Boko Haram en Nigeria y los filiales del Sahel como el Grupo de Apoyo al Islam y los Musulmanes (JNIM), etc. Estas zonas de conflicto se convirtieron en verdaderos caldos de cultivo de radicalización y yihad armada, donde el componente local se fusionaba con una narrativa transnacional de guerra santa contra el enemigo lejano ("*far enemy*") y el enemigo cercano ("*near enemy*") (Hegghammer, 2010).

Este proceso fue favorecido por una creciente globalización de los discursos, donde el acceso a tecnologías de comunicación e internet permitió la difusión masiva de la narrativa yihadista. Las revistas digitales como Inspire, Dabiq o Rumiyah entre otras, no solo ofrecían contenidos ideológicos, sino que articulaban estrategias militares, justificaciones teológicas y manuales para realizar atentados, convirtiéndose en auténticos instrumentos y manuales de adoctrinamiento y movilización de nuevos combatientes para su causa (Winter, 2017).

Paralelamente, los cambios geopolíticos tras la Primavera Árabe (2011) exacerbaron el vacío de poder en países como Siria, Libia o Yemen, dando lugar a contextos extremadamente propicios para la instalación de células terroristas. En estos escenarios de fragmentación institucional y guerra civil, las organizaciones yihadistas no solo encontraron refugio, sino la oportunidad de presentarse como alternativa de orden y justicia, estableciendo estructuras de poder basadas en una interpretación rigorista y fundamentalista de la sharía.

El ejemplo más paradigmático fue la proclamación del Califato por parte del autodenominado Estado Islámico, en adelante Daesh, en 2014. Su expansión relámpago por amplias regiones de Siria e Irak no solo modificó la geopolítica regional, sino que reconfiguró la naturaleza del reclutamiento yihadista, ya que, por primera vez desde los años del Emirato Talibán, se ofrecía una tierra gobernada según el islam radical, una "utopía" para la umma donde miles de combatientes, hombres, mujeres y menores, acudieron desde más de 80 países. Se estima que al menos 40.000 combatientes extranjeros se desplazaron a Siria e Irak entre 2012 y 2017 (Soufan Center, 2017), una cifra sin precedentes en la historia del terrorismo moderno.

Este fenómeno transnacional, con ramificaciones digitales, religiosas y políticas, exige un análisis riguroso de su génesis, pero también de sus implicaciones a largo plazo. Como advierte Vidino (2015):

Los yihadistas que viajan al extranjero no son únicamente un problema externo; cuando regresan, traen consigo experiencia militar, conexiones internacionales y una visión más radicalizada del mundo, lo que

convierte su retorno en uno de los principales desafíos de seguridad para Europa.

La figura del combatiente extranjero, *foreign terrorist fighter*, en adelante FTF, según la terminología empleada por Naciones Unidas, se ha consolidado como uno de los ejes estratégicos del yihadismo transnacional contemporáneo. A diferencia del muyahidín clásico que participaba en una guerra local, el nuevo combatiente yihadista no viaja solo para luchar, sino que también para integrarse en un proyecto ideológico y político: la creación de una comunidad islámica global regida por la sharía.

El informe del Soufan Group (2015) identificó tres perfiles predominantes entre los combatientes europeos: jóvenes de segunda generación de inmigrantes musulmanes, conversos sin vínculos previos con el islam, y sujetos con antecedentes penales comunes. Estos perfiles evidencian que la radicalización no responde exclusivamente a variables religiosas, sino a una amalgama de factores identitarios, psicológicos, sociales y emocionales. En muchos casos, el desplazamiento a Siria o Irak fue percibido como un acto de redención, pertenencia y propósito vital. En este mismo sentido, el fenómeno de las mujeres combatientes también ha adquirido gran visibilidad. Aunque minoritarias en número, su rol no se limitó a funciones domésticas o sentimentales, pues han adoptado muchas ocupaciones dentro del entramado yihadista, reclutadoras, vigilantes de la moral pública o incluso como mártires suicidas. Como señala Torres (2020), "el Daesh supo otorgar a la mujer un espacio simbólico dentro del Califato, explotando su función en la perpetuación generacional del proyecto yihadista".

Una de las consecuencias más inquietantes del retorno de estos individuos es el riesgo de contagio ideológico y la posibilidad de comisión de atentados en suelo europeo. España, aunque no figura entre los países más afectados en cifras absolutas, ha registrado la vuelta de más de un centenar de radicalizados procedentes de Siria e Irak, en su mayoría integrados en Daesh. Según el entonces ministro del Interior, Jorge Fernández Díaz, en 2015 se contabilizaban 115 desplazados desde España hacia zonas de conflicto, de los cuales más del 75% de estos individuos fueron captados a través de Internet entre los años 2013 y 2016. Tras ello, una parte significativa fueron abatidos en zona de conflicto y otros

lograron retornar posteriormente, obligando a activar medidas específicas de vigilancia y desradicalización (Fernández, 2015; Reinares y García-Calvo, 2016). De estos, una parte fue detectada y procesada gracias a la aplicación del artículo 575.2 del Código Penal, que tipifica como delito el entrenamiento pasivo con fines terroristas (BOE, 2015).

Sin embargo, pese a que la cifra española de retornados es inferior a la de países como Francia, Bélgica o Reino Unido, no es desdeñable, ya que el retorno no solo implica el riesgo de reactivación violenta, sino también el desafío procesal de probar su implicación directa en actividades terroristas cometidas en el extranjero, cuestión que frecuentemente se ve obstaculizada por la falta de cooperación internacional o la inexistencia de pruebas materiales. Tal como advierten Reinares y García-Calvo (2016), uno de los principales retos que plantean los retornados reside en su “difícil detección y evaluación del nivel real de peligrosidad, especialmente en contextos urbanos donde se diluyen fácilmente entre entornos familiares o comunitarios”.

En efecto, muchos de estos individuos no regresan con la intención inmediata de cometer atentados, sino como potenciales agentes de reclutamiento, adoctrinamiento o financiación, lo que exige una respuesta integral que combine inteligencia preventiva, medidas judiciales y programas de desradicalización. Además, la amenaza que representan se multiplica cuando regresan con capacidades adquiridas en combate, adiestramiento en el uso de armamento, conocimientos de propaganda digital y vínculos transnacionales, lo que los convierte en vectores especialmente sensibles para la reactivación de células durmientes o la articulación de nuevos focos de radicalización.

5.4. ESPAÑA EN EL RADAR DEL YIHADISMO GLOBAL

Desde los atentados del 11 de marzo de 2004 en Madrid, España se ha consolidado como objetivo prioritario del terrorismo yihadista, tanto simbólica como operativamente. Aunque los ataques del 11M marcaron un punto de inflexión en la percepción social e institucional del fenómeno, lo cierto es que la amenaza ya se venía gestando desde la década de 1990, cuando se desmantelaron

las primeras células vinculadas al Grupo Islámico Armado (GIA) argelino y a Al Qaeda en territorio español (Vidino, 2019; Reinares, 2014).

La posición geoestratégica de España como puente entre Europa y el Magreb, su pasado histórico como al-Ándalus (frecuentemente reivindicado en la literatura yihadista), y su condición de Estado miembro activo en coaliciones internacionales contra el terrorismo, la han convertido en un blanco constante en los discursos de grupos como Al Qaeda y Daesh (Jordán, 2019). Prueba de ello son los constantes llamamientos para atacar suelo español vertidos en publicaciones como Inspire, Dabiq o Rumiyah, así como en vídeos de Al-Andalus Media Foundation (2016), la productora de Al Qaeda en el Magreb Islámico (AQMI), en donde aparecía el yihadista melillense Abu Al Nur Andalusi, comandante de la khatiba al-Quds (AQMI) quien ha vertido reiteradamente amenazas contra intereses españoles. En uno de sus vídeos difundidos en enero de 2016, un combatiente yihadista español proclamaba:

Hoy ellos están en nuestra tierra, en la tierra del islam, pero con el permiso de Dios llegará un día que nosotros conseguiremos pegarles en sus tierras, en Nápoles, en Roma, en Madrid, explosiones en todas partes con el permiso de Dios. (El Confidencial, 2016)

Como se puede observar la narrativa islamista radical no sitúa a España únicamente como “objetivo militar” por su participación en operaciones internacionales, sino como “territorio ocupado” que debe ser “recuperado”. Esta recuperación no es solo simbólica, sino que se proyecta en términos escatológicos y expansionistas, dentro de un marco de yihad ofensiva que busca restaurar el Califato. El propio Daesh, en uno de sus comunicados oficiales de 2015, afirmaba: “Volveremos a Al-Ándalus por la espada y con la bandera del Tawhid ondeando sobre sus fortalezas”.

Estas afirmaciones no deben tomarse como simples excesos retóricos, sino como indicadores de intención, tal y como ha subrayado Reinares (2021), quien advierte que la inclusión de España en los planes estratégicos de las organizaciones yihadistas no ha disminuido, sino que ha mutado hacia fórmulas más clandestinas, descentralizadas y digitalizadas. La amenaza ha dejado de centrarse

exclusivamente en ataques espectaculares tipo 11M y se ha desplazado hacia formas de violencia de menor escala, pero igualmente disruptivas, como los atentados con cuchillo, atropellos masivos o ataques individuales de inspiración salafista.

Además, la presencia continuada de ciudadanos españoles y residentes en España vinculados directa o indirectamente con los conflictos sirio-iraquí refuerza la convicción de que nuestro país no es ajeno a las dinámicas de captación, financiación, adiestramiento y propaganda del yihadismo global. Esta implicación no solo se manifiesta en el desplazamiento de combatientes a zonas de conflicto, sino también en el retorno paulatino de algunos de ellos, lo que ha planteado nuevos desafíos en términos de seguridad, reintegración y prevención del extremismo violento.

A este respecto, los últimos datos oficiales actualizados por el Ministerio del Interior revelan que, desde los atentados del 11 de marzo de 2004 hasta el 26 de mayo de 2025, España ha llevado a cabo un total de 1.176 detenciones por terrorismo yihadista, en el marco de 482 operaciones policiales. Solo entre 2022 y 2025 se han producido 265 detenciones, muchas de ellas relacionadas con la actividad de captación yihadista a través del ciberespacio, retornados de Siria e Irak, o con redes de financiación opacas (Ministerio del Interior, 2025). Las principales zonas de actuación siguen concentrándose en Cataluña, Madrid, Ceuta y Melilla, territorios donde convergen factores de vulnerabilidad social, radicalización ideológica y estructuras comunitarias susceptibles de instrumentalización por actores salafistas.

Por todo ello, la combinación entre amenaza externa (retornados, emisarios, captadores virtuales) y riesgo interno (actores locales, conversos, jóvenes vulnerables) configura un escenario de “radicalización sin fronteras” en el que las fronteras físicas resultan cada vez más porosas y el contexto digital se configura como un escenario crucial para sus intereses filoterroristas. Uno de los casos más paradigmáticos de radicalización fue el de Yassin Ahram Pérez, un joven nacido en Córdoba de madre española, quien viajó a Siria y se convirtió en un verdadero youtuber del Califato, difundiendo vídeos con amenazas directas contra España. En uno de ellos, pronunciado en castellano y acompañado por un menor (presuntamente su hijo), afirmaba: “Juro que, con la voluntad de Allah, conquistaremos España. Volveremos a Córdoba, a Toledo, a Sevilla... No

dejaremos un centímetro en manos de los cruzados. Y si no lo conseguimos, que mis hijos lo hagan...” (Onda Cero, 2017; El Espectador, 2017).

Este tipo de discursos ilustra con claridad el salto del yihadismo como fenómeno bélico al yihadismo como fenómeno comunicacional, viralizado mediante redes sociales, plataformas multimedia y foros cifrados. El caso de Ahram Pérez resulta especialmente alarmante porque conjugaba narrativas de guerra santa con elementos de identidad nacional, intentando apelar emocionalmente a jóvenes musulmanes españoles o conversos, muchos de ellos atrapados en procesos de desarraigo cultural o marginación social. Y es en este contexto, donde la figura del agente encubierto informático adquiere una importancia estratégica clave, ya que permite detectar, observar e infiltrarse en los entornos digitales, escenario predilecto para la difusión ideológica radical y la captación de nuevos adeptos.

**V – LA REVELACIÓN
ISLÁMICA FRENTE AL
ISLAMISMO POLÍTICO
TRANSNACIONAL**

V - LA REVELACIÓN ISLÁMICA FRENTE AL ISLAMISMO POLÍTICO TRANSNACIONAL

5.1. EL ISLAM COMO ÚLTIMO ESLABÓN DE LA CADENA PROFÉTICA

Desde su origen, el islam no se presenta como una religión nueva, sino como la culminación de un mensaje revelado progresivamente a través de los profetas anteriores, desde Abraham (Ibrahim) hasta Jesús (Isa), siendo Mahoma el “Sello de los Profetas.” (Corán, 33:40). Su aparición, a comienzos del siglo VII en la península arábiga, no solo representa la continuidad del linaje abrahámico, sino también la renovación de un monoteísmo que aspiraba a transformar de raíz tanto el orden espiritual como el social. La revelación recibida por Muhammad ibn Abd Allah, conocido como el Profeta Mahoma, se enmarca en un contexto tribal profundamente desigual, donde los valores de justicia, misericordia y comunidad eran sistemáticamente vulnerados por el poder oligárquico de los comerciantes de La Meca.

Mahoma, hombre de carácter contemplativo y sensibilidad social, solía retirarse a las montañas cercanas para meditar. Fue en una de estas ocasiones, hacia el año 610 d.C., cuando recibió en la cueva de *Hirá* la primera revelación de parte del arcángel Yibril: “¡Recita en el nombre de tu Señor que ha creado!, ha creado al hombre de sangre coagulada, y [...] ha enseñado al hombre lo que no sabía” (Cortés, 2005, 96:1–5).

Desde ese momento, la revelación coránica se prolongaría por 23 años en los que fue memorizada y recitada por sus compañeros hasta su muerte, no siendo hasta la época del Califa Uthman cuando se recopiló y fijo por escrito el texto coránico estructurándose en 114 capítulos o suras, de distinta extensión y tono. En sus inicios, durante el llamado “periodo mequí”, el mensaje del Profeta era profundamente espiritual y social, centrado en un Dios único, misericordioso y justo: “El Misericordioso, ha enseñado el Corán” (Cortés, 2005, 55:1). El mensaje también denunciaba sin ambages la injusticia y la arrogancia de los ricos hacia los huérfanos y mendigos:

Es liberar a un esclavo, o dar de comer, en un día de hambre, a un huérfano cercano, o a un pobre que se arrastra por el polvo.

Y ser de los que creen, que se recomiendan mutuamente la paciencia y se recomiendan mutuamente la misericordia. Éstos son los de la derecha.

Pero los que no creen en nuestros signos son los de la izquierda. El Fuego cerrará sobre ellos. (Cortés, 2005, 90:13–20)

No obstante, a medida que su predicación ganaba adeptos, especialmente entre los pobres, esclavos y sectores marginados de la sociedad mequí, también crecía el recelo y la hostilidad de las élites tribales, en particular del clan de los Quraysh. Para estos últimos, el mensaje de Mahoma no solo representaba una amenaza espiritual al politeísmo tradicional en la Región, sino una subversión directa del orden socioeconómico establecido, basado en los privilegios de linaje, el control de las caravanas comerciales y la administración del santuario de la Kaaba. Las tensiones alcanzaron un punto crítico cuando Mahoma denunció públicamente las injusticias sociales, el acaparamiento de la riqueza y el culto a ídolos paganos. Como consecuencia de ello, los líderes de La Meca comenzaron una campaña de persecución sistemática: presiones familiares, torturas, boicots económicos y amenazas de muerte. Tal como recogen diversas fuentes islámicas como la Sira de Ibn Ishaq o las crónicas posteriores de Al-Tabari, se llegó a conspirar directamente contra la vida del Profeta, organizando un plan para asesinarlo durante la noche mientras dormía en su casa.

Ante esta situación de peligro inminente, Mahoma decide huir en secreto junto a su compañero más cercano, Abu Bakr. La huida hacia Yatrib (conocida actualmente como Medina), ciudad oasis situada al norte, se produjo en el año 622 d.C. y sería conocida como la Hégira (Hijra), término que en árabe significa 'emigración'. Este evento no solo marca el traslado físico del Profeta, sino el nacimiento de una nueva comunidad político-religiosa, la umma o comunidad de creyentes, cimentada en la fe islámica. La Hégira representa así una ruptura

histórica y espiritual con el tribalismo árabe, y por ello se adopta como el punto de partida del calendario islámico, el año 1 de la era musulmana.

Instalado como árbitro en Medina, Mahoma asume un rol dual: guía espiritual y líder político-militar. Los suras medinenses reveladas en esta etapa desarrollan un cuerpo legal cada vez más complejo, regulando aspectos como la guerra, la herencia, el comercio o la convivencia intercomunitaria: “¡Oh creyentes! No os está permitido heredar a las mujeres contra su voluntad” (Cortés, 2005, 4:19).

La llamada Constitución de Medina, si bien discutida por algunos autores como Aslan (2005), sienta las bases de la comunidad islámica (umma) como una entidad supra tribal que reconoce a Mahoma como profeta y árbitro. La pertenencia a esta comunidad ya no depende del linaje, sino de la adhesión a la *shahada*¹: “No hay más dios que Allah, y Mahoma es el mensajero de Dios”.

Durante este periodo, Mahoma emprende múltiples campañas militares, legitimadas no solo por la necesidad de proteger a la joven comunidad islámica frente a amenazas externas, sino también como mecanismo para asegurar recursos, consolidar alianzas tribales y extender la nueva fe. Estas acciones se encuadran en un contexto donde la guerra era una práctica estructural del tejido político de la Arabia preislámica, pero adquieren una nueva dimensión al estar refrendadas por revelaciones consideradas de origen divino. Tal es el caso de la sura de la Vaca, donde se establece el principio del *qital*, la lucha armada en defensa de la comunidad, como un acto no solo lícito, sino necesario en determinadas circunstancias: “Combatid por Allah contra quienes os combatan, pero no os excedáis. Ciertamente, Allah no ama a los transgresores (Cortés, 2005, 2:190).”

Este mandato establece un marco ético de la guerra, delimitando el uso legítimo de la violencia dentro de parámetros religiosos, lo que posteriormente dará lugar a la compleja doctrina de la yihad armada, que desarrollaremos posteriormente.

A partir de aquí, y bajo su liderazgo como *qa'id* (caudillo), el islam establece los cimientos de un orden normativo que trasciende la religión para devenir en

¹ La Shahada es el primer pilar del islam y la declaración de fe fundamental, que se traduce como “No hay más dios que Allah, y Mahoma es el mensajero de Dios”. Es la afirmación de la unidad de Dios (tawhid) y la aceptación de Muhammad como su profeta y último mensajero.

sistema jurídico-político. Las disputas con las tribus judías, que se negaron a reconocer su autoridad religiosa, acentuaron la separación entre las religiones del Libro y consolidaron la identidad islámica. La oración cambió su orientación de Jerusalén hacia La Meca, y se estructuraron los cinco pilares del islam: *Shahadā* (profesión de fe), *Salah* (obligatoriedad de realizar las oraciones diarias), *Zakat* (limosna), *Sawm* (ayuno durante el Ramadán) y *Hajj* (peregrinación a La Meca al menos una vez en la vida y si las condiciones de salud lo permiten).

Sin embargo, más allá de los pilares, la consolidación doctrinal del islam se materializó en un sistema normativo integral conocida como *sharīa*, literalmente “camino hacia el manantial”, que recoge el conjunto de normas, valores y preceptos derivados de la revelación coránica y de la Sunna, la tradición profética. A diferencia del cristianismo, donde la ley civil y la fe pueden escindirse, en el islam toda la vida del creyente, desde lo ritual hasta lo jurídico, queda supeditada a la esfera religiosa.

Por otro lado, tenemos la *Sunna* que recoge las acciones, palabras y aprobaciones tácitas del Profeta Mahoma, conservadas a través de los *hadices*, dichos y hechos del profeta. Esta fuente secundaria del derecho islámico adquirió una importancia mayúscula al complementar y contextualizar los mandatos del Corán. Obras como las de al-Bujari o Muslim, reconocidas entre las seis compilaciones canónicas del islam sunní, han sido objeto de rigurosos criterios de autenticidad (*isnād y matn*) para garantizar su fiabilidad (Esposito, 2016).

A partir de ambas fuentes se desarrolla el *fiqh*, es decir, la jurisprudencia islámica, que, a través de métodos de interpretación como el *qiyas* (analogía), el *ijma'* (consenso) y el *ijtihad* (esfuerzo interpretativo), permite aplicar los principios divinos a situaciones nuevas. Así, se establecen normativas sobre derecho penal, herencia, familia, comercio o relaciones internacionales. En este contexto, la *sharīa* no constituye un código cerrado, sino un sistema dinámico cuyo alcance depende de la visión particular que le otorguen las diferentes escuelas jurídicas dentro del islam, unas más beligerantes que otras: hanafí, malikí, shafi'í y hanbalí (Hallaq, 2009).

Desde esta perspectiva, se establecieron conceptos como el *dar al-Islam* (territorio del islam) y el *dar al-harb* (territorio de guerra), categorías jurídicas que influirían profundamente en la teorización posterior sobre la legítima defensa y la expansión de la umma, así como en el desarrollo doctrinal de la yihad.

Este carácter totalizador donde lo jurídico, lo moral y lo espiritual se entrelazan distingue al islam de otras religiones monoteístas. La umma, como comunidad de creyentes, se convierte en un cuerpo político-religioso guiado no por una autoridad sacerdotal, sino por la ley revelada. Esta visión integral del islam, como “*da'wa*” (religión y Estado), configuró una civilización que durante siglos irradiaría una visión normativa teocéntrica, pero también profundamente jurídica, que aún hoy determina las legislaciones de muchos países del mundo musulmán.

5.2. MOVIMIENTOS ISLAMISTAS TRANSNACIONALES: TRADICIÓN, POLÍTICA Y RELIGIÓN.

A lo largo del desarrollo histórico del islam, desde la muerte del Profeta hasta nuestros días, los pilares doctrinales sobre los que se asienta esta fe, la sharía, la sunna y el Corán, han sido objeto de múltiples interpretaciones por parte de ulemas, imanes, teólogos y pensadores. Estas reinterpretaciones no han permanecido confinadas al plano espiritual, sino que han influido decisivamente en la configuración de ideologías político-religiosas que, en no pocos casos, han servido como justificación teológica para la violencia yihadista. Tales lecturas han trazado también los marcos éticos en los que se apoyan manuales operativos contemporáneos de los grupos terroristas más radicales.

En el actual contexto de globalización, donde los mensajes se expanden a través de plataformas digitales y redes transnacionales, los movimientos islamistas han adquirido una dimensión mundial. Entre ellos, el más influyente, cuando no el más determinante en la configuración del islamismo moderno, es sin duda el de los Hermanos Musulmanes (Yama'at al-Ijwan al-Muslimun), matriz ideológica de buena parte de las organizaciones político-religiosas actuales, incluidas las organizaciones terroristas yihadistas contemporáneas.

5.2.1. Los Hermanos Musulmanes

Desde su fundación en 1928 por Hassan al-Banna, los Hermanos Musulmanes (HHMM) (*Yamaat al-Ijwan al-Muslimun*) se han erigido como el

principal movimiento islamista transnacional contemporáneo, caracterizado por una cosmovisión integral que amalgama lo religioso, lo político y lo social bajo la égida de la sharia. Definidos por Ortega (2012) como “la primera organización islámica reformista de alcance mundial, que pretendía un cambio social global”, los HHMM surgieron en un Egipto convulso, fracturado entre la secularización forzada por las élites y el desarraigo identitario que generaban las influencias coloniales.

Bajo un lema que condensaba su ideario revolucionario “Allah es nuestro objetivo; el Corán nuestra Constitución; el Profeta nuestro líder; la yihad nuestro camino y la muerte en la causa de Allah, nuestra más alta aspiración” (Castaño, 2013), la Hermandad planteaba la reislamización de la sociedad como proyecto integral para la civilización. Inspirado en el salafismo y la sunna, al-Banna pretendía reconstituir el Califato y devolver al islam su centralidad normativa. La influencia inicial del sufismo, que impregnó su pensamiento espiritual, fue gradualmente sustituida por un discurso más militante conforme tomaba conciencia del retroceso político del islam frente al secularismo kemalista y al dominio colonial británico.

Ya en 1938, la Hermandad se había consolidado como fuerza política de masas, captando apoyos en universidades, sindicatos y barrios obreros. Sin embargo, su auge no estuvo exento de controversia. El asesinato de Mahmud Fahmi al-Nasqrasi y las tensiones con el gobierno egipcio desencadenaron su disolución formal en 1954, lo que no impidió su supervivencia como estructura clandestina. El propio al-Banna fue asesinado en 1949, dejando un movimiento huérfano, pero ideológicamente fortalecido, en el que comenzaban a despuntar nuevos referentes como Sayyid Qutb.

El crecimiento exponencial del movimiento de los Hermanos Musulmanes durante las décadas de 1930 y 1940 llevó aparejado el diseño de una estructura orgánica sólida, pensada para resistir la represión estatal y garantizar su expansión tanto a nivel local como internacional. La organización fue formalizada por Hassan al-Banna en 1945 mediante la Ley Fundamental de la Sociedad de los Hermanos Musulmanes, que definía su jerarquía y división funcional. Desde entonces, dicha arquitectura apenas ha sido modificada.

En la cúspide del organigrama se sitúa el Guía Supremo (al-Murshid al-‘Āmm), máxima autoridad religiosa y política, que preside tanto el Consejo General

de Guía como la Asamblea Consultiva (Majlis al-Shura). Esta figura, elegida para mandatos renovables de seis años, debe ser varón musulmán, mayor de 30 años, con al menos cinco años de militancia activa, y una conducta moral intachable. A su vez, la Asamblea elige al secretario general y al tesorero, y supervisa los distintos comités funcionales: legal, financiero, político, etc. (Al-Banna, 1945, citado en Castaño, 2013, p. 121).

La base operativa de la organización reside en las células llamadas *usras* (familias), pequeños grupos de diez miembros que forman clanes, batallones y redes sociales insertadas en barrios, mezquitas, universidades o centros de asistencia social. Esta red celular descentralizada facilita tanto la acción social como el adoctrinamiento religioso y político, reproduciéndose en todos los países donde los HHMM han logrado implantarse.

No obstante, el verdadero punto de inflexión en la configuración estructural del movimiento fue la creación en los años 40 de la Sección Especial o Secreta (al-Nizām al-Khāṣṣ), también conocida como al-Nizām al-Sirrī. Inicialmente subordinada a al-Banna, esta sección fue concebida para coordinar las acciones de autodefensa frente al colonialismo británico y el sionismo. Sin embargo, con el tiempo funcionaría con creciente autonomía, convirtiéndose en un aparato paramilitar dentro del movimiento (Martín, 2011, p. 203).

Su existencia fue confirmada tras la incautación de documentos y manuales durante redadas estatales, los cuales revelaban un programa de adoctrinamiento intensivo. Los reclutas, extraídos de círculos deportivos y juveniles, eran formados bajo consignas como “Soldados del Misericordioso” y “el arte de morir”, culminando con un juramento a modo de ritual: “Con el Corán en la mano derecha y un arma en la izquierda”, pronunciaban su lealtad ciega a Allah y a la Hermandad, con los ojos vendados. Este modelo de iniciación ha sido replicado por numerosos grupos yihadistas contemporáneos.

Al margen de esta sección, todo nuevo integrante debía también realizar un juramento general de fidelidad a la organización:

Me comprometo con Dios, el Más Alto, el Más Grande, a unirme firmemente al mensaje de los Hermanos Musulmanes, a combatir por él, a vivir según las reglas de sus miembros, a tener confianza plena en su jefe y a obedecerle totalmente y en toda circunstancia, sea ésta afortunada o desgraciada [...]. (Al-Banna, 1945, citado en Ortega, 2012, p. 97)

Esta estructura interna ha sido exportada y adaptada en países como Francia, Alemania, España o el Reino Unido, donde los HHMM operan mediante asociaciones culturales, mezquitas, ONGs y plataformas políticas. Siguiendo el modelo egipcio, también han reproducido la lógica de las usras, actuando como agentes de islamización comunitaria y como brazo ideológico de la umma transnacional.

Respecto a su concepción de Estado, los Hermanos Musulmanes postulan un modelo de gobierno islámico regido por la sharía, estructurado en cuatro poderes: ejecutivo (controlado por el gobernante), legislativo (compartido con el Consejo de Shura), judicial (independiente y sometido a la ley islámica) y financiero. El Corán es concebido como Constitución, y la legitimidad del gobierno se basa en la consulta (shura) y el consenso popular.

Según Muhammad al-Ghazali (1917–1996), otro de sus ideólogos, las sanciones penales como la flagelación, la amputación o la lapidación solo se aplicarían en una sociedad plenamente islamizada, donde el Estado garantice primero la justicia social y económica. Esta doctrina revela el carácter condicional del castigo en el islam político, pero también su eventual legitimación según el grado de islamización alcanzado (Al-Ghazali, 1990, citado en Castaño, 2013, p. 137).

En resumen, los Hermanos Musulmanes presentan una doble faz: una estructura comunitaria asistencial que promueve la educación, el bienestar y la representación política de los musulmanes; y un núcleo ideológico e incluso paramilitar que promueve, cuando lo estima necesario, la acción violenta para imponer un sistema islámico integral. Esta dualidad de movimiento reformista y fuerza subversiva ha marcado su devenir y explica por qué muchas de sus ideas

han servido de matriz para la génesis de sus ideólogos más beligerantes, como es Sayyid Qutb, y cuyos dogmas se han convertido en fuente de inspiración yihadista.

La evolución del pensamiento de Sayyid Qutb (1906–1966) constituye una inflexión ideológica de primer orden dentro de los Hermanos Musulmanes y, por extensión, del islam político moderno. Intelectual egipcio formado en pedagogía y literatura, Qutb fue inicialmente un pensador moderado, colaborador del Ministerio de Educación egipcio y defensor de una renovación cultural basada en la fe (Kepel, 2001, p. 52). Sin embargo, su estancia en Estados Unidos entre 1948 y 1950 marcaría un punto de no retorno. Pues, durante su tiempo en Occidente, Qutb quedó profundamente impactado por lo que consideraba “una sociedad moralmente degenerada, individualista, racista y materialista” (Berman, 2003, p. 21). Esta experiencia generó en él un rechazo visceral hacia el modelo occidental moderno, al que consideraba incompatible con los valores islámicos, por lo que, a su regreso a Egipto, se unió a los Hermanos Musulmanes, alineándose con los postulados de su ala más radical y distanciándose del reformismo pacífico (Vidino, 2010, p. 48).

Durante su encarcelamiento bajo el régimen de Gamal Abdel Nasser, donde fue brutalmente torturado (Kepel, 2001, p. 62), Sayyid Qutb escribió sus obras más influyentes: *Fi Zilal al-Qur'an* (A la sombra del Corán), (Justicia social en el islam) y *Ma'alim fi al-Tariq* (Jalones en el camino), esta última considerada por diversos autores como el manifiesto fundacional del islamismo yihadista contemporáneo (Calvert, 2010, p. 123). En estas obras, Qutb sistematizó una cosmovisión radicalmente dicotómica del mundo, dividida entre el dar al-Islam (la tierra del islam) y el dar al-harb (la tierra de la guerra), negando cualquier posibilidad de coexistencia ideológica o neutralidad (Gerges, 2005, p. 27).

Sumado a ello, uno de los conceptos centrales en su pensamiento fue la relectura del término *jahiliyya*, usado tradicionalmente para describir el periodo preislámico de ignorancia y paganismo y su aplicación a las sociedades contemporáneas, incluso aquellas de mayoría musulmana que no se regían íntegramente por la sharía. Para Qutb, estas sociedades estaban sumidas en una nueva ignorancia espiritual, jurídica y cultural. Como él mismo sostiene:

La sociedad en la que vivimos es una sociedad de jahiliyya. Sus ideas, sus conceptos, sus costumbres, sus tradiciones, su cultura, sus leyes, su arte, su literatura... todo es producto de la jahiliyya. (Qutb, 1964, p. 18)

[...] No es la forma del gobierno lo que determina si una sociedad es islámica o jahiliyya; lo que importa es la fuente de la legislación. Si la fuente es Allah, entonces la sociedad es islámica; si no, es jahiliyya, aunque todos sus miembros se proclamen musulmanes. (Qutb, 1964, p. 51)

Esta acusación se convierte, de facto, en una justificación para el *takfir*², es decir, la excomunión de gobernantes y ciudadanos que no apliquen estrictamente la sharía. Para Qutb, la jahiliyya no es un estado neutral o meramente cultural, sino una agresión activa contra el islam. En sus propias palabras: "El objetivo del islam no es únicamente destruir el sistema jahili, sino reemplazarlo por un sistema islámico completo. No hay espacio para coexistencia entre ambos. El islam debe imponerse y eliminar a la jahiliyya" (Qutb, 1964, p. 84).

Este planteamiento fue especialmente explotado por ideólogos yihadistas contemporáneos más reputados como por ejemplo, Ayman al-Zawahiri, quien en *Knights Under the Prophet's Banner* adoptó la retórica de Qutb al afirmar que "la jahiliyya moderna ha superado incluso a la anterior en su corrupción y amenaza para el alma humana" (al-Zawahiri, 2001). Osama Bin Laden, quien en su carta a América afirmaba que: "Rechazáis la sharía de Allah para seguir vuestras propias leyes, inventadas por vosotros mismos, según vuestros deseos y caprichos. Esto es una apostasía de la religión de Allah y una rebelión contra Él" (Bin Laden, 2002), o Abu Musab al-Suri (2005) quien en su obra *Llamamientos a la resistencia islámica global* afirma que "el estado de jahiliyya permite el uso de la violencia no solo como defensa, sino como purificación".

² Musulmán que es acusado de apóstata.

En definitiva, esta conceptualización de la jahiliyya como una situación permanente y ubicua, junto a los postulados de los ideólogos anteriormente mencionados, ha permitido a los grupos yihadistas contemporáneos, Al-Qaeda y Daesh, justificar tanto el terrorismo interno en países musulmanes como la expansión globalista del mismo en occidente, al definir como infieles , y por tanto combatibles, a casi todos los gobiernos existentes. Esta radicalización semántica del término lo convierte en una herramienta de deslegitimación absoluta de cualquier orden político no islámico.

5.2.2. El Hizb Ut-Tahrir Al-Islami (HuT)

El Hizb Ut-Tahrir Al-Islami (Partido de la Liberación Islámica), más conocido como HuT, constituye uno de los movimientos islamistas sunníes más estructurados, doctrinalmente coherentes y radicales desde el punto de vista ideológico en la escena global. Fundado en 1953 en Jerusalén por Taqiuddin an-Nabhani, antiguo miembro de los Hermanos Musulmanes, juez del tribunal de apelación de Al-Quds y profundo conocedor de la jurisprudencia islámica clásica, HuT emergió en un contexto convulso: la humillante derrota árabe en la guerra de Palestina en 1948, el asesinato de Sayyid Qutb en Egipto y la consolidación del modelo secular nacionalista impulsado por regímenes como el de Gamal Abdel Nasser (Baran, 2004).

Aunque no registrado como partido político en ninguna legislación nacional, Hizb ut-Tahrir se presenta en sus propios documentos como una entidad política de alcance global: “Somos un partido político cuya ideología es el islam, por lo que la política es su trabajo y el islam su ideología” (Hizb ut-Tahrir, 2001, p. 7).

Desde sus orígenes, el objetivo central del movimiento ha sido la reinstauración del Califato islámico como forma de gobierno única y legítima, según lo ordenado por el Corán, la Sunna del Profeta y las prácticas de los *sahaba* (los compañeros del Profeta). El califa, en este sistema, no es un mero jefe de Estado, sino el vicario de Dios en la Tierra, encargado de gobernar conforme a la sharía. Tal como sostienen sus textos doctrinales: “El islam ha sido revelado para dominar

sobre todas las demás formas de vida. Este es el objetivo: establecer el dominio del islam en todo el mundo, mediante la llamada pacífica o, si es necesario, mediante la yihad” (Hizb ut-Tahrir, 2001, p. 20). Por todo ello, el HuT se opone frontalmente a la democracia representativa, a la soberanía popular y al modelo liberal-capitalista, al considerar que éstos usurpan la soberanía que, según su visión, solo pertenece a Dios (hakimiyya): “Mientras el sistema capitalista reclama la soberanía para la humanidad, el sistema islámico la reclama para Dios. Esta es la diferencia esencial” (Al-Nabhani, 1998, p. 51).

A diferencia de otros movimientos islamistas que combinan pragmatismo con dogma, Hizb ut-Tahrir mantiene una postura rígidamente doctrinaria, afirmando que no participará en instituciones democráticas ni en regímenes que no reconozcan el dominio de la ley divina, aunque sí utilizará medios pacíficos y legales para propagar su mensaje y dismantelar el “sistema de *kufr*³” imperante.

En lo que respecta a su estrategia expansiva, el HuT adopta una metodología tripartita inspirada en el itinerario del Profeta Muhammad desde La Meca a Medina:

La primera etapa, conocida como Tatbiq al-thaqafa (fase de aculturación ideológica) consiste en formar una élite doctrinal altamente capacitada en los fundamentos del islam político. No se trata simplemente de transmitir conocimientos religiosos, sino de forjar cuadros militantes con una cosmovisión integral y combatiente. Como sostiene el propio an-Nabhani: “No enseñamos el islam como una teoría académica, sino como un proyecto de vida a implementar sobre la tierra” (Al-Nabhani, 1999, p. 5). Las obras clave que conforman este proceso formativo incluyen *The System of Islam*, *The Islamic Personality* y *The Ruling System in Islam*, donde se trazan todos los aspectos que debería asumir un Estado islámico bajo liderazgo califal.

En esta etapa inicial, los miembros del partido se agrupan en pequeños núcleos o células, *halqa*, formadas por no más de cinco personas, lo que permite preservar la clandestinidad y evitar la infiltración. Cada célula se encuentra supervisada por un *mushrif* (instructor), quien mantiene contacto únicamente con

³ Infieles.

su superior jerárquico inmediato, replicando una estructura organizativa de inspiración leninista, basada en compartimentos estancos (Baran, 2004, p. 11).

La segunda fase, denominada tafa'ul ma'a al-umma (interacción con la sociedad), tiene como objetivo generar una masa crítica de apoyo social y cultural hacia el Califato. El partido despliega entonces su activismo mediante conferencias, publicaciones, campañas en redes sociales, y contactos con élites políticas, religiosas y militares. An-Nabhani insiste en que “es obligación luchar políticamente contra los regímenes impíos hasta que se sometan a la autoridad de Allah” (Al-Nabhani, 2002, p. 147). Esta etapa no solo busca la diseminación doctrinal, sino también el desgaste de la legitimidad de los gobiernos vigentes. Se cultiva así una narrativa de oposición radical, fomentando un clima de disidencia que preceda a la ruptura institucional.

Durante esta etapa, Hizb ut-Tahrir refuerza su presencia en universidades, centros culturales islámicos y redes juveniles, especialmente entre jóvenes musulmanes que viven en contextos occidentales donde la identidad religiosa se percibe como amenazada. Según el Counter Extremism Project (2023), “la captación ideológica se centra en estudiantes, profesionales y conversos, con especial atención a quienes muestran desafección al sistema liberal-democrático o frustración identitaria”.

Cabe destacar que en algunos países del continente europeo, como Reino Unido o Alemania, el HuT ha utilizado de forma estratégica las libertades de expresión y asociación para expandir su ideario, aprovechando el marco jurídico democrático que en otros lugares combate abiertamente. En palabras de Towsen (2022), “el partido proyecta una imagen moderada en contextos hostiles, pero mantiene intacta su matriz totalitaria, bajo el principio de *taqiyya*⁴ o disimulación doctrinal” (p. 96).

⁴ La *taqiyya* es una técnica o forma preventiva de ocultación, que permite a los fieles la negación de sus creencias y prácticas religiosas. Esta característica adoptada principalmente por la confesión chiíta para protegerse de sus perseguidores, también ha sido extrapolada a las organizaciones islamistas radicales sunitas como forma de consecución de sus objetivos, a fin de poder pasar desapercibidos en occidente.

Finalmente, la tercera etapa, conocida como *istilām al-ḥukm* (toma del poder), se reserva para el momento en que se haya alcanzado una masa crítica doctrinalmente formada y una red de aliados estratégicos en las élites civiles y militares. Aunque HuT afirma que esta transición debe ser pacífica, su ambigüedad histórica ha sido señalada por varios informes de seguridad. En efecto, ha sido vinculado con intentos fallidos de golpe de Estado en Jordania (1969), Uzbekistán (2004) y Tayikistán (2005), lo que ha motivado su proscripción en muchos países de Asia Central (Human Rights Watch, 2004).

Una vez instaurado el Califato, HuT propone una forma de gobierno teocrática regida exclusivamente por la *sharīa*. Todo pluralismo político desaparece, y la legitimidad emana directamente de Dios a través del califa. Este, según el Draft Constitution del partido, “ostenta el poder supremo del Estado, incluyendo el mando militar, la emisión de leyes, el control económico y la política exterior, bajo supervisión del partido, pero sin fiscalización democrática” (Hizb ut-Tahrir, 2001, art. 26).

En relación con la política internacional, el Califato estaría obligado a expandir el islam globalmente mediante el *da’wa* (predicación) y, si es necesario, a través de la *yihad* armada. Así lo estipula an-Nabhani: “El islam debe imponerse en todo el mundo, por medio de la *yihad*, si no se acepta voluntariamente” (Al-Nabhani, 2001, p. 37). Por lo que, esta mezcla de legalismo, proselitismo y estructura celular convierte a HuT en un actor geoestratégico de primer orden dentro del yihadismo político global.

Esta dimensión global ha permitido su establecimiento en múltiples regiones del mundo, especialmente en aquellos países con significativa presencia musulmana. Sin embargo, es en Europa y Asia Central donde su proyección política y doctrinal ha generado mayores tensiones, tanto por sus métodos de implantación como por la ambigüedad de su mensaje respecto a la violencia.

En el caso europeo, el HuT ha desarrollado una sofisticada red de proselitismo dirigida fundamentalmente a jóvenes musulmanes, tanto de origen inmigrante como conversos, que experimentan un proceso de desarraigo o marginación identitaria. Utilizando una narrativa de confrontación con el sistema liberal-occidental, la organización promueve una identidad musulmana “pura” basada en la superioridad de la *sharīa* como única fuente legítima de normatividad. Como afirma el Counter Extremism Project (2023), el HuT “presenta el islam como

una alternativa integral al sistema democrático, ofreciendo una identidad fuerte y estructurada frente al vacío moral de Occidente”.

En este contexto, países como Alemania prohibieron oficialmente el partido en 2003, acusándolo de promover “ideologías contrarias al orden constitucional” y de difundir mensajes antisemitas y antidemocráticos (MEMRI, 2003). Rusia, China, Egipto, Pakistán, Indonesia, Bangladés o Tayikistán han seguido esta misma línea, destacando la preocupación común ante un movimiento que, si bien no ejecuta directamente atentados, sí proporciona el andamiaje ideológico para legitimar la violencia. El Reino Unido, tras múltiples intentos fallidos, finalmente proscribió a HuT como organización terrorista en enero de 2024. Según la Home Office, la decisión se justificó por el hecho de que el partido “fomenta el odio, promueve la violencia y busca reemplazar los Estados democráticos por un Califato global” (UK Government, 2024).

Pese a su proscripción en numerosos países, HuT continúa operando a través de organizaciones pantalla, asociaciones culturales y plataformas digitales. Su capacidad de adaptación a los marcos legales vigentes le ha permitido mantener presencia activa en foros universitarios, medios alternativos y redes sociales. El International Centre for Counter-Terrorism (2022) señala que “la narrativa de HuT comparte estructuras ideológicas con los movimientos yihadistas violentos, pero encubierta bajo un barniz discursivo legalista y doctrinal”. En efecto, la frontera entre el islamismo político no violento y el extremismo violento resulta, en su caso, deliberadamente difusa.

En lo que respecta a España, la presencia de Hizb ut-Tahrir se remonta a 2004, con un foco especial en Cataluña. Según Jordán y Tarrés (2007), el grupo llegó a contar con una célula activa en Sabadell y desarrolló actividades de difusión ideológica a través de conferencias, mesas redondas, seminarios, manifestaciones, reparto de panfletos y, especialmente, foros de internet. Estas plataformas digitales, en su mayoría cerradas y accesibles solo por invitación, sirvieron como espacio de adoctrinamiento doctrinal y de contacto con otras filiales del partido en Reino Unido, Países Bajos y Marruecos.

Uno de estos foros de habla hispana fue desmantelado en 2007 tras la detención de varios de sus administradores, que estaban presuntamente vinculados a tareas de propaganda radical. Tal y como relatan los autores, la estrategia comunicativa de HuT se basa en el rechazo explícito de la democracia, considerada incompatible con el islam, y en la promoción del Califato como sistema político alternativo y totalizante. En consecuencia, su mensaje está dirigido a jóvenes musulmanes que muestran desencanto hacia el sistema liberal, apelando a su identidad religiosa y a la necesidad de restaurar la sharía (Jordán y Tarrés, 2007).

A pesar de declarar públicamente su rechazo a la violencia como método de acción, el HuT mantiene una postura ambigua respecto al uso de la fuerza. En múltiples ocasiones, sus portavoces se han negado a condenar explícitamente atentados como los del 11-S, el 11-M o el 7-J en Londres. En palabras del portavoz danés Fadi Abdellatif: “Ve a ayudar a tus hermanos en Faluya y extermina a tus gobernantes si obstaculizan tu camino” (citado en Vidino, 2010, p. 161). Este tipo de declaraciones ha motivado procesos judiciales en países europeos y ha reforzado la imagen de HuT como incubadora ideológica del extremismo, pese a su fachada legalista.

Hechos que se suman a que numerosos de sus integrantes han acabado engrosando las filas de organizaciones terroristas. Es el caso de Omar Bakri, quien tras su paso por HuT fundó al-Muhajiroun, grupo vinculado al terrorismo islamista en el Reino Unido. También Akram Yuldoshev, fundador del IMU (Movimiento Islámico de Uzbekistán), o incluso Abu Musab al-Zarqawi, quien posteriormente lideraría Al-Qaeda en Irak. Aunque el HuT insiste en desvincularse de estas trayectorias, la coincidencia doctrinal en la idea de la *hakimiyya* absoluta, el rechazo a la democracia y la abolición del Estado-nación lo sitúan en el mismo marco teológico que las organizaciones terroristas globales.

En definitiva, Hizb ut-Tahrir representa un ejemplo paradigmático de cómo un movimiento puede actuar como puente doctrinal entre el islamismo político y el extremismo violento. Su estructura jerárquica, su metodología gradualista y su cosmovisión totalizadora configuran una amenaza ideológica que, si bien se articula sin armas, sí que adoctrina en los postulados más rigoristas, radicaliza y prepara el terreno para aquellos que decidan pasar a la acción. Su presencia en España y Europa no puede medirse exclusivamente por atentados cometidos, sino

por su capacidad de moldear mentalidades y erosionar los cimientos del pluralismo democrático desde una ortodoxia teocrática y absolutista.

**VI – CORÁN Y ESPADA:
LA APROPIACIÓN
YIHADISTA DEL MENSAJE
DIVINO**

VI -CORÁN Y ESPADA: LA APROPIACIÓN YIHADISTA DEL MENSAJE DIVINO

6.1. LA YIHAD: DE MANDATO ESPIRITUAL A ESTRATEGIA TERRORISTA

Desde sus orígenes, el término yihad ha albergado una complejidad semántica que ha sido objeto de interpretaciones múltiples, muchas veces contradictorias. Derivado de la raíz árabe *jahada* que significa “esforzarse” o “luchar”, el concepto de yihad no nació con una connotación estrictamente militar, sino como una forma de esfuerzo, tanto espiritual como físico, en el camino de la sumisión a Dios, Allah. Así lo sugiere una tradición atribuida al Profeta Mahoma, recogida en compilaciones no canónicas como la de al-Nasa’i, que reza: “Hemos regresado de la pequeña yihad (la guerra) hacia la gran yihad, la lucha contra el alma”. Este pasaje, si bien discutido por parte de la ortodoxia hadítica, ha sido utilizado como referente ético en muchas corrientes sufíes y moderadas del islam.

Esta distinción entre la llamada yihad mayor (al-jihād al-akbar) y la yihad menor (al-jihād al-asghar) ha sido objeto de elaboración por parte de pensadores clásicos como al-Ghazali (1058–1111), quien afirmaba que “la verdadera batalla del creyente es contra la arrogancia del ego”, y por Ibn Qayyim al-Jawziyya (1292–1350), quien diferenció claramente entre una yihad espiritual, de purificación interna, y una yihad bélica, únicamente justificable en contextos de agresión contra la umma.

Sin embargo, el islam clásico no excluyó por completo el componente militar. Como señala el Corán en la aleya 2:190: “Combatid en el camino de Allah a quienes os combaten, pero no os transgredáis. Dios no ama a los transgresores”, se establece un principio de proporcionalidad que rigió históricamente las guerras del Profeta en Medina. Del mismo modo, el Corán exhorta a la prudencia en asuntos de guerra: “Si se inclinan hacia la paz, inclínate tú también” (Cortés, 2005, 8:61). Esta ambigüedad permitió que el concepto de yihad pudiera ser entendido como lucha defensiva legítima, pero también, con el tiempo, susceptible de reinterpretación en clave ofensiva o política.

Durante los primeros siglos del islam, juristas como al-Mawardi (972–1058) o Ibn Khaldun (1332–1406) codificaron la yihad como una obligación colectiva (*fard kifāyah*) de la comunidad musulmana, a ejercer bajo liderazgo legítimo y dentro de normas éticas de la guerra. Estas prescripciones, aunque normativas en su tiempo, fueron poco a poco perdiendo su sentido originario en favor de lecturas más radicales que instrumentalizaron el concepto con fines ideológicos.

Con el paso del tiempo, y especialmente a partir del siglo XX, esta tensión entre espiritualidad y militarismo fue explotada por pensadores islamistas que vieron en la yihad un instrumento revolucionario. Tal es el caso de Sayyid Qutb, quien en su célebre obra *Hitos en el camino* (*Ma'alim fi-l-Tariq*), convirtió la yihad en el núcleo de su programa político. “La yihad no es un movimiento defensivo. Es una acción destinada a eliminar todos los obstáculos que impidan a los hombres aceptar el islam por voluntad propia” (Qutb, 2006, p. 61). Para Qutb, el mundo moderno se hallaba sumido en una nueva jahiliyya, una ignorancia comparable a la de la Arabia preislámica, y solo mediante la yihad se podría restablecer la soberanía de Dios sobre la tierra.

Esta interpretación es profundamente revolucionaria, pues transforma la yihad de una obligación puntual y colectiva, limitada a contextos de legítima defensa, en una obligación individual y permanente (*fard ‘ayn*) contra todo sistema secular o gobierno considerado apóstata. Tal planteamiento supone un giro teológico de enorme calado: ya no se lucha para defender a la umma, sino para instaurar un nuevo orden islámico global.

La expansión de esta visión ha sido impulsada por figuras como Abul A'la Maududi y posteriormente por ideólogos como Abu Muhammad al-Maqdisi o Abu Musab al-Zarqawi, quienes asumieron que el mundo entero estaba sumido en el error y la idolatría, legitimando así la yihad ofensiva incluso contra gobiernos musulmanes. Este viraje doctrinal se resume en una frase de al-Maqdisi (2005): “Es obligatorio realizar la yihad contra los infieles hasta que se sometan a la voluntad de Allah”. Esta evolución doctrinal nos permite advertir cómo una noción inicialmente espiritual fue reformulada, primero por teólogos clásicos y luego por ideólogos radicales, hasta convertirse en uno de los ejes vertebradores del islamismo político contemporáneo.

6.2. LA EXEGESIS VIOLENTA DEL CORÁN Y SU LEGITIMACIÓN PARA EL COMBATE

En la medida en que el concepto de yihad evolucionó desde una dimensión interior hacia una praxis armada, el texto coránico fue objeto de una exégesis que justificaba el uso de la violencia como mandato religioso. Algunas de estas exégesis han priorizado la dimensión pacífica y espiritual del mensaje coránico, mientras que otras, particularmente aquellas adoptadas por movimientos salafistas-yihadistas, han derivado hacia una lectura belicista, que justifica el uso de la violencia como mandato divino y permanente. Esta relectura radical, alejada de la tradición hermenéutica clásica del *tafsir*⁵, configura un marco doctrinal donde la yihad menor (al-jihād al-aṣghar) adquiere centralidad como obligación personal (fard ‘ayn), independientemente del contexto histórico que rodea a las revelaciones.

Uno de los versículos más recurrentes en la propaganda yihadista es la aleya 9:5, conocida como "la aleya de la espada", revelada tras la ruptura de pactos entre los musulmanes y tribus politeístas: "Y cuando hayan pasado los meses sagrados, matad a los asociados donde los encontréis, capturadlos, sitiadlos y tendedles emboscadas" (Corán, 9:5). Este versículo, que en su marco original respondía a la traición política de ciertos clanes árabes, ha sido elevado por los ideólogos del yihadismo a la categoría de versículo abrogador (*naskh*), con capacidad para anular más de un centenar de aleyas que promovían el diálogo, la clemencia o la cohabitación interreligiosa (Spencer, 2006, p. 48). Doctrinarios como Abu Muhammad al-Maqdisi (2005) y Anwar al-Awlaki reinterpretaron esta aleya como un mandato universal, desligado de su contexto histórico, y en consecuencia aplicable a todo no musulmán que se niegue a someterse al dominio político de la sharía.

Otro pasaje clave utilizado por estos movimientos es la aleya que reza: "Se os ha prescrito el combate, aunque os repugne; puede que detestéis algo que sea

⁵ Exégesis o interpretación del Corán, es decir, el estudio detallado y comentado del texto coránico con el fin de comprender su significado profundo, contexto histórico y aplicación jurídica o espiritual.

bueno para vosotros, y que améis algo que sea malo para vosotros. Dios sabe, y vosotros no sabéis” (Cortés, 2005, 2:216).

Originalmente vinculada a las guerras defensivas en Medina, esta aleya ha sido descontextualizada para afirmar que el combate no solo es deseable, sino obligatorio, incluso si provoca rechazo emocional. Tal formulación ha servido como base doctrinal para justificar la participación armada de jóvenes musulmanes en conflictos de Siria, Irak o Mali, presentando la violencia como vía de expiación y elevación espiritual (Torres, 2017, p. 44).

La beligerancia textual se intensifica en la aleya que declara: “Infundiré el terror en los corazones de los que no creen; golpead sus cuellos y golpead cada uno de sus dedos” (Cortés, 2005, 8:12).

Revelada en el marco de la batalla de Badr, la primera gran confrontación militar entre musulmanes y la tribu de Quraish, esta aleya es una de las más instrumentalizadas por el aparato mediático del Daesh. En ella se justifica no solo la violencia física, sino su teatralización, sirviendo como base teológica para atrocidades como las decapitaciones públicas. El número 4 de la revista Dabiq lo expresa con crudeza: “El islam no reconoce ningún derecho a los infieles mientras no se sometan a la autoridad de Allah” (Dabiq, 2014, p. 10).

Desde esta óptica, no solo se legitima la agresión contra los considerados *kuffār*, sino también contra aquellos musulmanes que colaboran con sistemas políticos democráticos o rechazan la imposición de la sharía. Es lo que se denomina *takfir*, o excomunión activa, un principio que permite atacar incluso a correligionarios bajo la acusación de apostasía. En definitiva, el salafismo yihadista ha convertido el Corán en una herramienta de guerra, descontextualizando sus versículos y aplicándolos como dogma de acción inmediata y obligatoria para la realización de la yihad (Reinares y García-Calvo, 2013).

Finalmente, cabe señalar la influencia doctrinal de líderes como Abu Bakr al-Baghdadi, quien, en su célebre discurso en Mosul, en 2014, proclamaba ante miles de fieles: “El islam no es una religión de paz. Es una religión de combate” (Rumiyah, nº 1, 2016, p. 11).

Con estas palabras, no solo se legitimaba la violencia, sino que se glorificaba como camino superior al del pacifismo, como forma de restaurar la dignidad de la umma y vengar los agravios sufridos por el islam.

La progresiva institucionalización del combate en el mensaje coránico queda patente en suras donde el creyente es definido por su entrega abnegada al esfuerzo bélico: “¡Luchad por Dios como Él se merece! [...] ¡Él es vuestro Protector! ¡Es un protector excelente, un auxiliar excelente!” (Cortés, 2005, 22:78).

Aquí no se alude a la guerra en términos defensivos o excepcionales, sino como un deber moral que define la identidad misma del musulmán. La apelación a Abraham, figura patriarcal del monoteísmo, enmarca esta lucha como continuidad de una tradición sacralizada. Tal formulación ha permitido a grupos como Al Qaeda establecer una narrativa de restauración profética, donde la violencia no es una desviación sino un retorno al islam “auténtico” (Firestone, 1999, pp. 131–132).

Del mismo modo, otras aleyas refuerzan la equivalencia entre fe verdadera y disposición al combate: “Son creyentes únicamente los que creen en Dios y en Su Enviado, sin abrigar ninguna duda, y combaten por Dios con su hacienda y sus personas. ¡Ésos son los veraces!” (Cortés, 2005, 49:15).

Este versículo fue esgrimido en los sermones de Anwar al-Awlaki para despreciar a los musulmanes moderados, tachándolos de hipócritas e infieles encubiertos. La violencia, bajo esta lógica, no solo es permisible, sino prueba de fe. La radicalización opera aquí como un proceso de exclusión: solo quien combate, cree.

La rigidez doctrinal se acentúa cuando se abordan las reticencias al combate. El Corán responde a los objetores de la guerra mediante una condena moral: quienes se niegan a combatir son equiparados con los incrédulos, tal como recoge la aleya 3:167: “Se les dijo: ‘¡Vamos! ¡Combatid por Dios o rechazad al enemigo!’ Dijeron: ‘Si supiéramos combatir, os seguiríamos’. Aquel día estaban más cerca de la incredulidad que de la fe...” (Cortés, 2005, 3:167).

Este reproche coránico, dirigido a quienes se abstuvieron de participar en la batalla de Uhud, es reinterpretado por los salafistas como advertencia atemporal contra el pacifismo o la neutralidad. Los textos exegéticos de Ibn Taymiyya ya anticipaban esta interpretación al identificar el abandono del combate como signo de debilidad espiritual (Ibn Taymiyya, 2010, pp. 42–44).

Además, aleyas como la 2:217: “Combatir en el mes sagrado es pecado grave, pero apartar del camino de Dios lo es aún más” (Cortés, 2005, 2:217), buscan desacralizar las antiguas treguas tribales del calendario árabe preislámico, dando prioridad absoluta a la lucha por la fe. Esta disposición, convertida en argumento legal por los juristas hanbalíes, refuerza la idea de que no existe tiempo ni lugar en el que el combate esté vedado si la causa es divina.

Por su parte, el versículo 4:76–77 no solo legitima el enfrentamiento con los enemigos del islam, sino que califica como traidores a quienes temen al enemigo más que a Dios: “Quienes creen, combaten por Dios. Quienes no creen, combaten por los taguts. Combatid, pues, contra los amigos del Demonio” (Cortés, 2005, 4:76).

Esta polarización entre fieles guerreros y aliados del demonio ha sido clave en la propaganda visual de Daesh, que ha retratado a sus enemigos —tanto occidentales como musulmanes moderados— como servidores del *shayṭān*⁶, recurriendo a iconografías apocalípticas (Lesaca, 2017, pp. 92–97).

En la aleya 9:29, el mandato se extiende incluso contra los “gentes del Libro”: “¡Combatid contra quienes, habiendo recibido la Escritura, no creen en Dios ni en el último Día [...] hasta que, humillados, paguen el tributo directamente!” (Cortés, 2005, 9:29).

Este versículo, que forma parte del mismo corpus revelado que la aleya de la espada, ha sido central en la doctrina de imposición del *jizya* —tributo obligatorio a los no musulmanes— y ha sido empleado por grupos como Boko Haram o el Estado Islámico para justificar la sumisión de cristianos y yazidíes bajo su dominio (Nance y Sampson, 2017).

Finalmente, cabe destacar la aleya 2:190–193, donde se establece un umbral entre la violencia legítima y la desmesura: “Combatid por Dios contra quienes os combatan [...] pero no os excedáis. Dios no ama a los que se exceden” (Cortés, 2005, 2:190).

La interpretación clásica imponía aquí límites éticos al uso de la fuerza. Sin embargo, los yihadistas modernos eluden esta contención argumentando que, al

⁶ Satanás.

tratarse de una guerra defensiva de la umma contra una agresión global, cualquier exceso está justificado como represalia o disuasión (Qutb, 1964, p. 314).

La aleya 22:39–40 es uno de los primeros pasajes que introduce la noción del combate justificado por agresión previa. El texto dice: “Les está permitido a quienes son atacados, porque han sido tratados injustamente [...] A quienes han sido expulsados injustamente de sus hogares, sólo por haber dicho: ‘¡Nuestro Señor es Dios!’...” (Cortés, 2005, 22:39–40).

Esta formulación inicial de la yihad defensiva ha sido reinterpretada por teóricos del salafismo yihadista para legitimar campañas militares contra regímenes musulmanes seculares, bajo la premisa de que estos “expulsan a los verdaderos creyentes” y obstaculizan el establecimiento de la sharía. Abu Muhammad al-Maqdisi (2004) argumenta que este versículo otorga carta blanca para alzarse contra todo orden político que no reconozca el islam como fuente única de legislación.

A su vez, el Corán 9:38 denuncia la tibieza de los creyentes que rehúsan ir a la guerra: “¿Por qué, cuando se os dice: ‘¡Id a la guerra por la causa de Dios!’, permanecéis clavados en tierra? ¿Preferís la vida de acá a la otra?” (Cortés, 2005, 9:38).

Esta apelación retórica aparece repetidamente en sermones de al-Baghdadi, quien llamaba a sus seguidores a abandonar sus países para unirse al Califato, acusando de hipocresía (nifaq) a quienes se aferraban al confort occidental (Rumiyah, nº 1, 2016, p. 11). El concepto de la hégira, abandono del “dar al-kufr” hacia el “dar al-islam”, se vincula aquí con el cumplimiento efectivo de la yihad ofensiva.

La aleya 8:39, por su parte, establece como objetivo último del combate el sometimiento global a la autoridad islámica: “Combatid contra ellos hasta que dejen de induciros a apostatar y se rinda todo el culto a Dios” (Cortés, 2005, 8:39).

Esta aleya ha sido la base para la formulación de una yihad global sin fronteras, en la que todo espacio que no se someta a la sharía es visto como legítimo campo de batalla (dar al-harb). Como advierte Kepel (2004), la universalización de

esta lógica bélica es lo que distingue al terrorismo yihadista contemporáneo del nacionalismo islámico tradicional.

Otro fragmento significativo es la aleya 9:73, donde se exhorta al Profeta a combatir no solo a los infieles, sino también a los hipócritas: “¡Combate contra los infieles y los hipócritas, sé duro con ellos! Su refugio será la gehena...” (Cortés, 2005, 9:73).

Esta indicación ha sido interpretada como justificación para atacar no solo a enemigos externos, sino también a los musulmanes moderados, chiíes o sunníes no radicales. Grupos como Daesh han usado esta aleya para declarar la guerra a organizaciones islámicas que consideran apóstatas, como los Hermanos Musulmanes o partidos islamo-demócratas, acusándolos de connivencia con el *kufur*.

En conjunto, estas aleyas ofrecen el corpus doctrinal que los ideólogos del yihadismo reinterpretan como mandato permanente de guerra. El discurso apocalíptico que suele acompañar esta exégesis se nutre del imaginario de las últimas batallas, donde el islam se enfrentará a las fuerzas de Occidente (Rumiyah, 2016; Dabiq, 2014). En ese marco escatológico, la violencia se eleva a sacramento redentor.

Esta lectura del Corán como texto de combate se vincula con una visión del mundo binaria y escatológica, donde el enemigo no es un actor político, sino un infiel ontológico que amenaza la existencia misma del islam. En palabras de Reinales y García-Calvo (2013), “la radicalización salafista como ideología, ha convertido la yihad como una obligación religiosa para varones capaces de ello” erigiendo la revelación divina en estrategia bélica, y al creyente en soldado eterno.

Así pues, el Corán ha sido transformado por los ideólogos del terrorismo yihadista en un texto de guerra permanente, una fuente legitimadora de violencia estructural, cuya aplicación se extiende no solo al campo de batalla físico, sino también al simbólico, jurídico y teológico. Esta instrumentalización de la palabra revelada constituye una de las distorsiones más alarmantes de la espiritualidad islámica en el siglo XXI.

6.3. DE AL-QAEDA A DAESH Y SU COSMOVISIÓN DE LA YIHAD COMO FORMA DE GUERRA GLOBAL

En el tránsito del siglo XX al XXI, la noción de yihad sufre una transformación doctrinal decisiva: pasa de ser un deber colectivo bajo autoridad legítima (*fard kifayah*) a convertirse en un mandato individual e incondicional (*fard 'ayn*). Este viraje fue teorizado inicialmente por figuras como Abdullah Azzam, mentor espiritual de Osama Bin Laden, quien ya en los años ochenta afirmaba que la yihad armada era una “obligación personal de cada musulmán, como lo eran el ayuno y la oración” (Azzam, 1987, p. 19). A partir de entonces, se asiste a una obligación divina que induce a la yihad como un sexto pilar del islam, y de esta forma se justifica cualquier forma de lucha, independientemente del contexto, del blanco o del método.

El punto de inflexión se produce en 1998 con la publicación de la fatwa del Frente Islámico Mundial para la Yihad contra los judíos y los Cruzados, firmada por Bin Laden y otros líderes yihadistas en la que se decreta: “Matar a los estadounidenses y a sus aliados civiles y militares es una obligación individual de todo musulmán capaz de hacerlo, en cualquier país en que se hallen” (World Islamic Front, 1998). Esta declaración inaugura un nuevo paradigma bélico, donde la yihad se transforma en una guerra sin fronteras, sin reglas y sin posibilidad de tregua. No es casual que tras esta fatwa se produjesen los atentados contra las embajadas de EE. UU. en Kenia y Tanzania (1998), el ataque contra el USS Cole (2000) y, finalmente, el 11-S en Nueva York y Washington (2001).

Al Qaeda elaboró así un marco teológico-militar en el que la violencia no es solo legítima, sino que se convierte en medio privilegiado de purificación del mundo. Como explican Reinares y García-Calvo (2014), “el discurso de Al Qaeda no es simplemente reactivo o defensivo, sino profundamente redentor: el islam debe imponerse como totalidad política y espiritual” (p. 22). La lógica binaria impuesta por la ideología de dar al-islam frente a dar al-harb cobra aquí una dimensión apocalíptica.

Este modelo fue recogido y llevado a su máxima expresión por Daesh a partir de 2014, con la proclamación del Califato Islámico por Abu Bakr al-Baghdadi.

A diferencia de Al Qaeda, que carecía de un territorio propio, Daesh consolidó un espacio físico sobre el que instauró su visión extrema de la sharía. El líder del grupo expresó en su primer sermón: “La yihad no se detendrá hasta que la tierra sea purificada de la inmundicia de la incredulidad... El Islam no es una religión de paz. Es una religión de combate” (Rumiyah, nº 1, 2016, p. 11).

Las publicaciones del Estado Islámico, como Dabiq y Rumiyah, profundizaron en este marco de violencia absolutista. En Dabiq nº 15, por ejemplo, se ofrece una guía detallada para perpetrar ataques individuales en Occidente a través de la selección de objetivos, uso de cuchillos o vehículos, y glorificación del martirio. Según Daesh, el verdadero creyente es aquel que actúa sin esperar órdenes, inspirándose directamente en el Corán y los hadices bélicos. Así, se invoca el versículo 8:60 como mandato permanente: “Y preparad contra ellos cuanto podáis de fuerza y de caballos atados para infundir terror en el enemigo de Dios” (Cortés, 2005, 8:60).

Este modelo descentralizado de yihad, desprovisto de jerarquías formales, dio lugar a una nueva figura operativa: el “lobo solitario” (lone wolf), idealizado por Rumiyah como paradigma del musulmán combatiente fiel en el camino de Allah: “Tú, el creyente oculto entre los infieles, eres el puñal de la umma. Actúa. No esperes órdenes. No esperes compañeros” (Rumiyah, nº 2, 2016, p. 17). Sumado a ello, los dogmas emitidos en sus publicaciones enfatizan en legitimar religiosamente la comisión de atentados terroristas en suelo europeo. Por ejemplo, en Dabiq nº 12 se invoca la aleya 47:4, “cuando os enfrentéis a los infieles, golpeadles el cuello”, para justificar las decapitaciones del Estado Islámico. Esta retórica de la violencia no se limita a un contexto bélico convencional, sino que abarca cualquier espacio considerado contaminado por la jahiliyya moderna: cafés, redacciones de prensa, estadios deportivos, salas de conciertos, iglesias, etc.

En suma, la estrategia doctrinal de Al Qaeda y Daesh ha logrado fijar una gramática del terror donde la yihad ya no es únicamente un esfuerzo por la fe, sino una obligación de martirio global, un deber indiscriminado de sangre, y una forma de espiritualidad deformada que confunde la salvación con el exterminio.

6.4. DEL FRENTE DE BATALLA AL CIBERESPACIO: LA YIHAD COMO INSURRECCIÓN DIGITAL DESCENTRALIZADA

El cambio de paradigma introducido por Al Qaeda y Daesh no solo implicó una transformación doctrinal sobre la legitimidad del uso de la violencia, sino también un cambio radical en el terreno desde el cual esta violencia se ejerce. Si en el siglo XX la yihad aún se pensaba como un fenómeno territorial vinculado a campos de batalla concretos (Afganistán, Bosnia, Chechenia), en el siglo XXI, y especialmente tras el auge de Internet y las redes sociales, esta adopta una dimensión completamente nueva: la del campo de batalla virtual. Aquí nace lo que los analistas denominan el neoyihadismo digital (Lorenzo-Dus y Macdonald, 2018), una modalidad insurgente que emplea la infraestructura de la red para formar, adoctrinar, coordinar y activar a individuos radicalizados en cualquier parte del mundo.

El ideólogo que mejor supo anticipar este viraje fue Mustafa Setmariam Nasar, más conocido como Abu Musab al-Suri, autor de una de las obras más influyentes dentro del panorama yihadista, Llamada a la resistencia islámica global. En esta obra de más de 1.600 páginas, al-Suri establece las bases de una nueva estrategia de yihad descentralizada, alejada de las estructuras jerárquicas convencionales, y más cercana a la lógica de guerrilla urbana de inspiración maoísta. Según él, “la yihad de nuestros tiempos debe ser global, descentralizada, oculta e ideológicamente cohesionada” (al-Suri, 2005, p. 1287).

Su propuesta consistía en formar individuos autosuficientes que pudieran ejecutar ataques sin necesidad de órdenes directas, recurriendo al entrenamiento doctrinal en línea y a manuales operativos distribuidos en foros y canales de mensajería. Esta concepción daría origen al modelo de los lobos solitarios, individuos radicalizados en la intimidad y anonimato del espacio digital, sin conexión formal con organizaciones terroristas, pero alimentados por su narrativa.

Este fenómeno se materializó en ataques como los de Madrid (2004), Londres (2005), París (2015) o Barcelona (2017), donde algunos de los implicados reconocieron haber sido inspirados por vídeos de predicadores salafistas radicales como Anwar al-Awlaki o por contenidos digitales de revistas como Inspire (Al

Qaeda) o Rumiyah (Daesh). Estas publicaciones ofrecen, además de justificaciones teológicas, instrucciones prácticas para fabricar explosivos caseros como el conocido como “madre de Satán”, las formas de ocultación de armas y cuchillos para realizar apuñalamientos masivos, atropellos masivos con vehículos, etc.

Un ejemplo relevante es Inspire, publicada por Al Qaeda en la Península Arábiga (AQPA), que en su primer número instruía a los musulmanes occidentales sobre “cómo construir bombas en la cocina de tu madre” (Inspire, 2010).

Daesh, por su parte, en Rumiyah nº 2, explica paso a paso cómo maximizar el impacto de un atropello masivo en mercados navideños o fiestas populares. Estas guías no son simples provocaciones, sino verdaderas plataformas de adiestramiento (Rumiyah, 2016).

En este marco, el ciberespacio deja de ser un instrumento de comunicación para convertirse en una trinchera ideológica y táctica. Las redes sociales como Telegram, Whatsapp, Facebook, X (Twitter), TikTok o incluso servicios de videojuegos como Roblox o Call of Duty, han sido utilizados por Daesh y sus simpatizantes para difundir propaganda, captar nuevos miembros, coordinar acciones y mantener viva la narrativa de una umma hostigada que se encuentra adormecida y perseguida por occidente.

Cabe subrayar que esta nueva fase presenta una enorme dificultad para los servicios de inteligencia y fuerzas de seguridad. La detección temprana del radicalismo ya no depende de estructuras observables, sino de señales difusas: cambios en los hábitos digitales, consultas en portales de doctrina islámica radical o yihadista, la participación en foros cerrados y privados, el enaltecimiento de mártires en la causa de Allah y sus ideólogos, etc. Como apunta Reinales (2015), “la yihad digital no requiere viajes ni contactos; solo una conexión a Internet y una convicción sólida, construida a través de un discurso uniforme y omnipresente” (p. 59).

El resultado es una yihad individualizada, atomizada, pero no menos letal. Tal como advirtiera el experto francés Gilles Kepel (2016), se trata de una “radicalización por contagio narrativo”, en la que la ficción apocalíptica del Califato, la injusticia global y la promesa de redención inmediata ofrecen a jóvenes alienados un marco épico desde el que destruir y, paradójicamente, darle sentido a su existencia.

Desde esta perspectiva, la amenaza contemporánea del yihadismo no se limita ya a campos de batalla lejanos, sino que se manifiesta con igual o mayor peligrosidad en los entornos digitales cotidianos, anónimos y deslocalizados. Este modelo híbrido que combina doctrina medieval, teología radicalizada, tecnologías modernas y narrativa de victimización global no solo prolonga el ciclo del terrorismo, sino que lo vuelve más difícil de contener. La yihad ya no se lanza desde una trinchera ni desde una mezquita: puede emerger desde un dormitorio juvenil, desde una cafetería con Wi-Fi, o desde el teclado de un adolescente que se radicaliza en silencio entre vídeos de YouTube y discursos de mártires.

Ante este escenario, cobra una especial trascendencia la figura del agente encubierto informático, concebido legalmente como una herramienta clave en la lucha contra las nuevas formas de radicalización. Su importancia no es solo táctica, sino también jurídica y estratégica. A través de este recurso procesal, previsto y regulado en la legislación penal española y que abordaremos en profundidad en los capítulos posteriores, permite a determinados agentes de las Fuerzas y Cuerpos de Seguridad infiltrarse en espacios digitales cerrados y controlados por estructuras yihadistas, observando, documentando y, lo que es aún más crucial, recolectando pruebas válidas que no solo permiten prevenir ataques, sino que también pueden ser aportadas con todas las garantías procesales ante un tribunal.

El valor del agente encubierto informático o digital radica precisamente en su capacidad de convivir entre los canales de difusión propagandística del terrorismo sin levantar sospechas, proporcionando acceso directo a entornos donde el discurso violento germina y se difunde. Así, no solo actúa como un instrumento de anticipación frente a posibles atentados, sino como una salvaguarda del orden jurídico, pues su presencia convierte lo efímero del ciberespacio en una constancia probatoria que puede ser analizada, valorada y utilizada en procesos penales, respetando siempre los principios de legalidad y proporcionalidad.

Además, en términos preventivos, esta figura permite detectar procesos de radicalización en sus primeras fases, antes de que se materialicen en acciones violentas. Gracias a su labor silenciosa y meticulosa, es posible trazar las redes de captación, identificar nodos de comunicación relevantes, y sobre todo, intervenir

en la fase ideológica del delito, cuando la mente del sujeto aún está en proceso de adoctrinamiento. En este sentido, no se trata únicamente de investigar o detener: se trata de preservar vidas, desactivar discursos letales y proteger la dignidad humana desde el conocimiento profundo del adversario.

**VII – USO DEL ENTORNO
DIGITAL POR PARTE DE AL-
QAEDA Y EL ESTADO
ISLÁMICO**

VII - USO DEL ENTORNO DIGITAL POR PARTE DE AL-QAEDA Y EL ESTADO ISLÁMICO

7.1. FORMAS DE RECLUTAMIENTO Y ADOCTRINAMIENTO A TRAVÉS DE PLATAFORMAS DIGITALES

En efecto, el paso del púlpito físico al ciberespacio supuso una transformación radical en las dinámicas de captación y adoctrinamiento. Las redes sociales, blogs, foros cerrados y plataformas audiovisuales como YouTube, Telegram o incluso videojuegos en línea, se convirtieron en auténticas escuelas virtuales de radicalización. La digitalización de la yihad permitió a los grupos terroristas proyectar una narrativa emocionalmente poderosa, tecnológicamente seductora y teológicamente legitimada.

El contenido producido no es improvisado, sino meticulosamente diseñado. Tal como demuestra el estudio de Mitts et al., (2022), las revistas como Dabiq o Rumiyah de Daesh emplean filtros visuales y técnicas de edición sofisticadas para magnificar el dramatismo de sus imágenes. Estas publicaciones manipulan el color, el contraste y la luz para dotar de aura heroica a los combatientes y representar a los enemigos del islam como figuras demoníacas, usando incluso efectos de “lens flare” para glorificar las armas de fuego como fuente de luz o redención.

A nivel técnico, esta estrategia también se observa en el uso de plataformas híbridas. Tras las intervenciones de Europol en 2018 y 2019 para dismantlar redes en Telegram, los grupos yihadistas no desaparecieron, sino que se adaptaron. Según el informe de Amarasingam et al., (2021), después del “Action Day” de 2019, la actividad yihadista en Telegram cayó drásticamente (un 94,7 % en publicaciones reenviadas), pero se multiplicó la creación de nuevos canales y la migración a plataformas alternativas como Rocket.Chat, TamTam, Hoop Messenger o Minds.com.

La resiliencia de estas redes demuestra que la propaganda yihadista no es simplemente doctrinal, sino también una operación técnica sofisticada, en la que los contenidos son replicados, reenviados y archivados mediante estructuras descentralizadas. Estas redes no solo instruyen; también generan pertenencia,

proyectan comunidad y cultivan una narrativa heroica destinada a jóvenes alienados, culturalmente desarraigados o en búsqueda de identidad.

Además, con la caída del califato físico, Daesh y Al Qaeda han intensificado sus esfuerzos por construir un califato virtual. Así lo revela el informe de la UE IRU (2018), que destaca el aumento exponencial de contenido generado por simpatizantes, especialmente durante fechas clave como Navidad, Semana Santa, eventos deportivos como el mundial de fútbol o protestas sociales como los *gilets jaunes* en Francia.

En esta etapa, las plataformas digitales ya no son meros medios de transmisión, sino auténticos espacios de socialización radical. Se pasa así de la propaganda a la participación activa, pues los jóvenes no solo consumen contenido, sino que interactúan, aportan, editan, subtitulan a sus respectivos idiomas e incluso diseñan campañas de violentas que circulan bajo etiquetas o hashtags compartidos o aparentemente inofensivos. Este viraje implicó también un cambio en el tipo del “potencial reclutado”, que ya no se centraría en el activista ideologizado que busca activamente el mensaje, sino el joven desorientado que lo encuentra de forma casual en medio de una estética audiovisual atractiva.

En este contexto, la utilización de videojuegos como Call of Duty, Roblox o Fortnite se ha documentado como canales indirectos de adoctrinamiento. En estos entornos, los “ciberreclutadores” observan las interacciones de usuarios jóvenes, evalúan su nivel de frustración o disconformidad social, e inician procesos de acercamiento mediante conversaciones aparentemente inocuas. Un informe de Europol (2022) confirmó la presencia de cuentas asociadas a Daesh en servidores de videojuegos, utilizadas para crear clanes afines, compartir enlaces a propaganda e incluso organizar sesiones privadas para distribuir vídeos de martirio o decapitaciones.

Este nuevo ecosistema digital ha favorecido la captación de adolescentes mediante técnicas de ingeniería emocional: se explotan sentimientos de marginación, discriminación o rabia mediante mensajes como “la umma te necesita” o “eres un soldado de Allah en territorio enemigo”. Como apunta Gil (2018, citado en Gazapo Lapayese, 2018), los individuos más vulnerables suelen ser jóvenes de segunda o tercera generación, especialmente aquellos con una identidad ambigua, nacidos en Europa pero excluidos simbólicamente de la ciudadanía plena. Estos sujetos, convertidos en “huérfanos simbólicos”, encuentran en la

narrativa del yihadismo no solo un enemigo común sobre el que enfocar su ira, sino una pertenencia, una identidad reconstruida a través del odio.

Todo ello, ha generado en el proceso de radicalización clásico un cambio de paradigma (McCauley y Moskalenko, 2008). Pues, una vez que los reclutadores identifican a aquellos sujetos más vulnerables o con mayor probabilidad de captación, hacen de gala de mecanismos como el contacto intenso directo, la generación de vínculos a través de la identificación diferencial con la causa, incluso comparten documentación, testimonios e información para una captación progresiva de sujetos hacia una radicalización violenta.

Según la investigación de Lodeiro, Oficial de la Guardia Civil:

Las nuevas tecnologías son uno de los factores estratégicos que han sabido explotar las organizaciones terroristas con multitud de finalidades, desde el reclutamiento, la propaganda, la financiación, el adiestramiento, la incitación o provocación a realizar acciones terroristas, hasta el acopio y difusión de información con finalidad terrorista [...] Siendo el principal fin perseguido por estas organizaciones terroristas, que con la radicalización de los jóvenes, éstos ejecuten una aportación a la causa a través de actos violentos, que en muchos casos les supondrá su propia muerte (Lodeiro, 2017).

Tal y como afirma Lesaca (2017), hemos dejado atrás el modelo de captación y adoctrinamiento clásico versado en una cercanía inmediata para dar paso a un modelo descentralizado cibernéticamente:

Antes, el modelo de captación y reclutamiento yihadista se sustentaba en el desplazamiento a los campos de refugiados o entrenamiento en zonas

controladas por la insurgencia, mezquitas o barrios donde existía una mayor tasa de marginalidad, y, por ende, jóvenes más desprotegidos. Sin embargo, ahora, las redes sociales se han convertido en el principal foco de captación y adoctrinamiento.

Resaltar que, el dominio online ofrece a los yihadistas según Weimann (2008) una serie de facilidades:

Acceso fácil, una gran audiencia potencial extendida por todo el mundo, anonimato en la comunicación, flujo rápido de información, interactividad, desarrollo barato, entorno multimedia y la habilidad de moldear la cobertura de la información de los medios de comunicación tradicionales, que utilizan Internet como fuente.

Como ya sabemos, las redes sociales se han convertido en un instrumento propagandístico, altamente eficaz. Las razones de su éxito entre los grupos terroristas yihadistas responden a varios factores (Illaro, 2015):

- Publicar en ellas es mucho más barato que en cualquier otro medio de comunicación convencional como radio, prensa o televisión.
- Su acceso no está centralizado y participar en ellos es fácil: sólo hace falta un dispositivo.
- Los mensajes pueden publicarse libremente, están exentos de los controles y políticas de publicación de los medios de comunicación convencionales.
- Su difusión geográfica es mayor que la que puedan alcanzar prensa, radio o televisión.
- Son inmediatos. No existe intervalo de tiempo entre el transcurso de un suceso y su narración en las redes

Sin embargo, el proceso de radicalización yihadista no puede comprenderse únicamente desde una perspectiva individual, psicológica o ideológica. Su verdadera complejidad emerge cuando se examinan las redes de pertenencia,

afecto e influencia en las que el sujeto se encuentra inserto. Tal y como han demostrado numerosos estudios contemporáneos, entre ellos los pioneros trabajos de Sageman (2004), la radicalización no es un fenómeno súbito ni solitario, sino un itinerario progresivo que se nutre del entorno relacional y digital del individuo, donde confluyen vínculos personales, narrativas simbólicas y mecanismos de socialización informal. En este contexto, las redes sociales, entendidas tanto en su vertiente interpersonal como en sus manifestaciones digitales, desempeñan un papel decisivo como plataformas de incubación ideológica, validación emocional y facilitación operativa.

Según Sageman (2004), aquellos individuos que cuentan en su entorno cercano con un militante yihadista ya sea en su familia o en su círculo de amistades, representan los ejemplos más paradigmáticos de este tipo de radicalización relacional. Sin embargo, más allá de esos casos prototípicos, se ha evidenciado que la participación activa en determinadas redes sociales puede ejercer un influjo gradual pero sostenido que conduce a la adopción de visiones extremistas. Este fenómeno no obedece únicamente a la transmisión doctrinal de ideas violentas, sino que responde a un entramado multifactorial, en el que las redes actúan como agentes de mediación simbólica, afectiva, material y organizativa. Así, la radicalización deviene menos una adhesión ideológica consciente y más un proceso de transformación identitaria influenciado por una diversidad de funciones que estas redes cumplen en el ciclo vital del sujeto. Pudiendo identificarse cinco dimensiones clave que explican su impacto en los procesos de captación y germen yihadista:

1. **Dimensión cognitivo-ideológica:** En una primera fase, las redes actúan como canales de exposición progresiva a creencias, marcos interpretativos y relatos simbólicos que permiten al individuo familiarizarse con la cosmovisión yihadista. Esta aproximación no siempre se realiza a través de discursos explícitamente violentos; por el contrario, suele iniciarse en entornos doctrinales más ambiguos, donde la crítica al mundo occidental, la defensa de un islam “puro” o el anhelo de un orden basado en la sharía se presentan como principios legítimos. Estas comunidades, centradas en figuras religiosas o asociaciones islamistas, funcionan como espacios de “presocialización ideológica”,

allanando el camino hacia doctrinas más militantes al compartir referentes salafistas, una orientación panislámica y una lectura exclusivista del islam. De manera aún más explícita, se difunden textos referentes a la jahiliyya moderna de Sayyid Qutb o ideas de predicadores como Anwar al-Awlaki, cuyas conferencias circulan masivamente en YouTube y Telegram, incluso tras su muerte, han combinado referencias doctrinales con una retórica de odio perfectamente adaptada al público occidental. Su influencia ha sido decisiva en atentados como el de Fort Hood (EE. UU., 2009) o en el proceso de radicalización de los hermanos Kouachi, autores de la masacre de Charlie Hebdo (BBC, 2015). Esta exposición doctrinal, progresiva y acumulativa, se convierte en un marco de interpretación global, donde el islam queda reducido a una narrativa de enfrentamiento apocalíptico.

2. **Dimensión socioemocional:** Más allá del contenido doctrinal, estas redes proporcionan al sujeto un ecosistema emocional que satisface necesidades de reconocimiento, pertenencia y validación. Jóvenes que atraviesan crisis identitarias, frustración vital o exclusión social encuentran en estas comunidades una narrativa que transforma el dolor en causa, y la soledad en hermandad. La radicalización, en este plano, no se explica tanto por la adhesión a ideas violentas, sino por el refugio emocional que estas redes ofrecen. En ellas, la autoestima se reconstruye sobre una épica de lucha y victimización, y la identidad personal se refuerza a través del vínculo colectivo. En palabras de Mustafa Setmariam, “la militancia islámica es también refugio emocional ante un mundo percibido como corrupto e hipócrita (2015). Esta dimensión emocional está ampliamente documentada en casos como el del joven belga Bilal Hadfi, participante en los atentados de París (2015), quien, había experimentado una ruptura identitaria tras sentirse marginado por su entorno escolar y social (Le Monde, 2015).”
3. **Dimensión instrumental o material:** Aunque no es el motor principal del proceso, no puede obviarse la función instrumental que algunas redes ejercen para ofrecer soluciones concretas a problemas materiales. Individuos desempleados, migrantes sin apoyo institucional o personas en situación precaria pueden encontrar en estas estructuras una fuente de ayuda económica, alojamiento, o incluso asistencia legal básica. Si

bien estas compensaciones rara vez son decisivas por sí solas, sí refuerzan la dependencia respecto al grupo y pueden actuar como incentivos que afianzan la lealtad o aceleran la entrega. En contextos marcados por la pobreza o el desempleo, como los barrios periféricos de Molenbeek en Bruselas o el suburbio de Trappes en París, se han detectado casos en los que la pertenencia a círculos islamistas ha proporcionado alojamiento, cobertura jurídica o incluso recursos económicos a jóvenes sin otra salida (El País, 2016). Estas ayudas fortalecen la dependencia del grupo y refuerzan su legitimidad ante los ojos del radicalizado.

4. **Dimensión de aproximación y captación:** La radicalización no culmina necesariamente en la violencia, pero cuando lo hace, suele ir acompañada de un paso ulterior: el contacto directo con estructuras terroristas. Este acercamiento puede ser buscado por el propio radicalizado o facilitado por reclutadores activos. En ambos casos, el nexo se produce dentro de redes ya frecuentadas por el individuo, ya sea en entornos físicos o digitales. Así, la adscripción a un grupo violento no aparece como un salto repentino, sino como el desenlace natural de una integración progresiva que ya ha moldeado su pensamiento y afectividad. En este sentido, la actividad de Mustafa Maya Amaya, converso al islam y residente en Melilla, representa uno de los ejemplos más significativos en el contexto español. Condenado en 2018 por liderar una red internacional de captación desde su domicilio, Maya mantenía contactos con Al Qaeda, el Estado Islámico y el Frente al-Nusra, valiéndose de herramientas como Facebook, Skype, Paltalk y foros privados en internet para atraer, adoctrinar y canalizar a cientos de jóvenes hacia Siria, Irak o Malí (El Confidencial, 2018). Su capacidad para operar desde una silla de ruedas, en una vivienda social, sin moverse físicamente de su entorno inmediato, revela la magnitud disruptiva del reclutamiento digital y la plasticidad de las redes de captación contemporáneas.
5. **Dimensión de control y consolidación:** Finalmente, una vez que el sujeto se incorpora a una organización o célula, la red cumple una

función de refuerzo interno. Los veteranos y miembros jerárquicamente superiores intervienen en la consolidación del neófito, tanto mediante la vigilancia de su conducta como a través de rituales, discursos o actividades que profundizan su compromiso ideológico. Este control simbólico, unido al aislamiento progresivo del entorno externo, afianza la identidad radical y dificulta cualquier retorno a la esfera social anterior. La red, en este punto, ya no es solo mediadora del proceso, sino su garante y ejecutora. Esta función ha sido ampliamente descrita en manuales internos de Daesh, que instruyen a los líderes sobre cómo mantener la lealtad del combatiente mediante aislamiento, tareas grupales y control emocional (ISIS Files, 2019). La radicalización, en este punto, se vuelve irreversible para muchos: se ha convertido en su única identidad posible.

A pesar de la abrumadora expansión del ciberespacio como escenario privilegiado para la radicalización y el reclutamiento, no puede afirmarse que los métodos tradicionales hayan desaparecido por completo. En realidad, lo que se observa es una convivencia de ambos, a veces solapada, a veces complementaria, entre las formas clásicas de captación de tú a tú y las nuevas estrategias digitales. Como señalan Miró y Moneva (2019), la criminalidad contemporánea tiende a manifestarse en una lógica dual, donde los actos pueden ejecutarse tanto en el espacio físico como en el virtual. En esta misma línea, Caneppele y Aebi (2017), advierten que ambos entornos no solo coexisten, sino que se refuerzan mutuamente, generando dinámicas híbridas que complejizan el fenómeno delictivo.

En este contexto, la elección de las organizaciones yihadistas por una propaganda visual y masiva no es casual. Se trata de una estrategia cuidadosamente diseñada para impactar emocional e ideológicamente en las audiencias. Como bien apunta Juan Orellana (2013) “el cine político y propagandístico poseen una gran facilidad para moldear la mentalidad del receptor e influir en su pensamiento y comportamiento”. Esta capacidad persuasiva se traslada hoy a los vídeos de ejecución, las infografías bélicas o los montajes épicos difundidos por Daesh y Al Qaeda, donde se articula un relato estético de la violencia que busca, de forma deliberada, seducir emocionalmente a los potenciales adeptos mediante una estética que glorifica la violencia y embellece

la muerte. Ejemplo de ello es la figura del mártir, que se presenta como héroe ejemplar de la umma, elevado a la categoría de modelo espiritual. Su sacrificio se edita con música épica, efectos cinematográficos y citas coránicas que construyen un relato mitificado del martirio, transformando el acto de morir en una promesa de eternidad, pertenencia y redención.

Esto explica que numerosos jóvenes vulnerables, expuestos a estos discursos en foros, canales de Telegram o redes sociales, no se perciban a sí mismos como meros espectadores. La representación constante de una comunidad combatiente, cohesionada y glorificada les permite sentirse parte activa de un movimiento global. Como advierte Collins (2014), este entorno simbólico y comunicativo hace posible que muchos de ellos se sientan respaldados para ejecutar todo tipo de actos en nombre de la yihad, convencidos de que forman parte de una lucha más amplia. En ese proceso, pueden evolucionar desde la mera simpatía hasta el adoctrinamiento activo, el apoyo financiero a las organizaciones terroristas, su incorporación formal a una célula operativa o incluso la comisión de atentados terroristas a costa de su propia muerte.

7.2. EVOLUCIÓN EN LA FINANCIACIÓN DEL TERRORISMO YIHADISTA

7.2.1. Mecanismos tradicionales de financiación

La financiación del terrorismo yihadista ha experimentado una profunda transformación desde las fuentes tradicionales hasta los métodos más sofisticados asociados al ciberespacio. Tanto Al Qaeda como Daesh han desplegado estructuras de financiación paralelas que combinan recursos provenientes de actividades ilícitas con otros de origen aparentemente legítimo, como las donaciones caritativas, el control de ONG o el uso de canales de transferencias informales. Esta hibridación constituye una de las mayores amenazas para la seguridad internacional, ya que permite alimentar células terroristas sin dejar rastros evidentes que puedan ser rastreados con los mecanismos clásicos de control financiero.

Al Qaeda, durante sus primeras décadas de existencia, se sostuvo gracias a una extensa red de benefactores privados, empresarios afines ideológicamente y

donaciones canalizadas a través de fundaciones islámicas. Uno de los canales más utilizados fue el zakat, el impuesto religioso que, al no estar sujeto a una regulación financiera estandarizada, permitió desviar sumas millonarias hacia la causa yihadista. Tal y como señala Antúnez (2022) “la ambigüedad entre ayuda humanitaria y financiación terrorista se ha aprovechado reiteradamente por organizaciones tapadera”. Las ONG, algunas de ellas registradas en países con legislación laxa en materia de transparencia contable, han servido como instrumentos clave para encubrir transferencias ilícitas destinadas a zonas de conflicto como Siria, Irak o Somalia.

Por su parte, Daesh representó una ruptura con el modelo financiero tradicional de Al Qaeda. Durante el auge de su “califato”, desarrolló un sistema económico autónomo basado en el control de recursos naturales, especialmente petróleo, la exacción de impuestos a la población local (*jizya*), el saqueo sistemático de bancos, el comercio ilícito de antigüedades y órganos, así como el secuestro con fines extorsivos. Tal como recuerda el informe de Europol TE-SAT 2024, “el modelo de financiación de Daesh integró una lógica protoestatal con mecanismos de coacción económica, control de aduanas, extorsión sistemática y redes de contrabando”.

A esta diversidad operativa debe sumarse una práctica constante: el blanqueo de capitales. Tanto en su vertiente instrumental como estructural, el lavado de dinero supone una amenaza al equilibrio del sistema financiero global. No solo contribuye al sostenimiento de redes terroristas, sino que erosiona la competitividad legal al permitir que ciertos actores económicos actúen con ventajas comparativas derivadas del uso de fondos ilícitos. Según Romera (2022), “el blanqueo distorsiona los fundamentos del mercado y debilita la confianza ciudadana en las instituciones democráticas”.

Entre los impactos económicos más relevantes destacan:

- El desplazamiento de estructuras productivas tradicionales en favor de empresas pantalla o vinculadas a redes criminales.
- La desestabilización del tipo de cambio por grandes transferencias de capitales ilícitos, que a su vez generan inflación, corrupción y pérdida de soberanía monetaria.
- La asignación ineficiente de recursos en función de criterios de opacidad y cobertura, más que por rentabilidad o impacto social.

- La desincentivación de la inversión extranjera legal ante el riesgo reputacional o la competencia desleal de capitales ilegales.

Estas dinámicas configuran un “capitalismo alternativo” que, lejos de ser residual, se convierte en un vector estructurante de las economías frágiles, principalmente en zonas de conflicto o bajo gobernanza débil. Las mafias y redes terroristas se insertan así en la economía global mediante mecanismos que, por su naturaleza, dificultan su trazabilidad. La convergencia entre financiación terrorista y crimen organizado, fenómeno conocido como “narcoterrorismo financiero”, encuentra en esta praxis su máxima expresión.

Asimismo, la consolidación de plataformas transfronterizas para la evasión fiscal y la falta de coordinación internacional eficaz —a pesar de los esfuerzos del GAFI— siguen generando brechas jurídicas y técnicas que permiten a estos grupos eludir sanciones, triangulaciones financieras y auditorías independientes.

Por último, el impacto del blanqueo no es sólo económico, sino también institucional. La debilidad de los mecanismos de control favorece la corrupción política, el clientelismo y la infiltración de elementos radicales en estructuras clave del aparato estatal. En este sentido, la lucha contra la financiación del terrorismo debe abordarse no sólo como una cuestión de seguridad, sino como una tarea esencial para preservar el Estado de Derecho, la equidad económica y la cohesión democrática en contextos vulnerables.

7.2.2. Financiación del terrorismo a través de medios digitales

Uno de los pilares fundamentales en la capacidad operativa de los grupos yihadistas como Al Qaeda y el autodenominado Estado Islámico ha sido su habilidad para financiar sus actividades a través de mecanismos innovadores, opacos y descentralizados. En la era digital, internet no solo se convirtió en un instrumento de propaganda, sino también en una infraestructura financiera alternativa que ha permitido a estas organizaciones obtener recursos sin necesidad de estructuras estatales o redes logísticas tradicionales.

En primer lugar, resulta destacable la progresiva adopción de criptomonedas como método preferente de transferencia de fondos. Su carácter seudónimo, descentralizado y su escasa trazabilidad para las autoridades tradicionales de control financiero han facilitado su uso en operaciones clandestinas. En enero de 2024, la Guardia Civil detuvo en Barcelona a un individuo vinculado a Daesh por utilizar múltiples direcciones de criptodivisas con fines de financiación terrorista (Ministerio del Interior, 2024, citado en Sánchez, 2024). Esta operación reveló la existencia de una red organizada que empleaba plataformas como Telegram para solicitar donaciones en Bitcoin y otras monedas de alto anonimato, simulando campañas humanitarias.

Más aún, informes del Grupo de Acción Financiera Internacional (GAFI) alertan del abuso del crowdfunding en la financiación del terrorismo islamista. Plataformas digitales inicialmente concebidas para proyectos sociales o culturales han sido utilizadas para encubrir transferencias monetarias con destino a zonas de conflicto, retornos de foreign fighters o adquisición de armamento (FATF/OECD, 2023). En muchos casos, estas campañas se camuflan tras causas humanitarias aparentemente legítimas, como la ayuda a huérfanos sirios o el envío de medicamentos, lo cual genera un importante dilema jurídico y operativo para los Estados.

En este contexto, organizaciones caritativas musulmanas reales o ficticias han desempeñado un rol decisivo. En palabras de Kohlmann (2006), estas estructuras ofrecen a los donantes una vía para contribuir “a la causa islámica” sin necesariamente tener conciencia de su verdadero destino. Torres (2020) documenta cómo webs vinculadas al Grupo Salafista para la Predicación y el Combate (GSPC) publicaban llamamientos directos a los “hermanos bendecidos por Alá con dinero”, animándolos a financiar la yihad desde la diáspora.

Por otro lado, el fraude digital constituye otra fuente relevante de ingresos. El ya célebre caso de Younes Tsouli, apodado “Irhabi 007”, puso en evidencia la capacidad de los ciberyihadistas para explotar vulnerabilidades informáticas, realizar estafas bancarias y vender datos robados en la dark web con el objetivo de financiar actividades terroristas (Ministerio del Interior, 2023, citado en Sánchez, 2024).

A esto se suma el uso del phishing, el ransomware y el pharming, técnicas que, combinadas con herramientas de inteligencia artificial generativa, potencian las capacidades de engaño de estas redes.

Especial atención merece la expansión de este fenómeno en plataformas FinTech y redes sociales, donde los grupos promueven campañas fragmentadas, anónimas, y con retórica religiosa, dificultando la identificación de los beneficiarios reales (FATF/OECD, 2023). Las criptomonedas de alto anonimato, como Monero o Zcash, y el uso de wallets fríos almacenados en dispositivos USB, hacen casi imposible rastrear los fondos sin colaboración internacional profunda y acceso a las claves privadas.

Además de la recaudación de fondos, los canales digitales han servido como plataforma para la venta de mercancías (desde ropa hasta productos digitales) en tiendas online afines, generando un flujo económico continuo. Tal como expone la UNODC, estas operaciones se articulan a través de comercio electrónico, transferencia electrónica de fondos, y donaciones dirigidas a ONGs pantalla, muchas veces registradas en países con legislación laxa o limitada cooperación judicial (UNODC, 2012, citado en Cano, 2011).

Por último, cabe destacar el papel de las economías ilícitas en zonas como el Sahel o Afganistán, donde la débil presencia estatal permite a organizaciones como Al Qaeda del Magreb Islámico o el Estado Islámico del Gran Sahara participar en contrabando de armas, trata de personas, y tráfico de drogas, incluyendo opio y metanfetamina. Estos recursos, si bien no están estrictamente vinculados al ciberespacio, son vehiculizados mediante sistemas de transferencia opaca como el hawala, en ocasiones reforzados por aplicaciones digitales de mensajería cifrada (El Qorchi, 2002; Sánchez, 2024).

Sin embargo, en el contexto actual de convergencia entre tecnologías de información y formas tradicionales de financiación, resulta imprescindible considerar mecanismos híbridos que, aunque no se perciban como sofisticados, siguen desempeñando un papel fundamental en el sostenimiento financiero de redes yihadistas. Las formas de pago como efectivo, cheques o transferencias acordadas fuera de sistemas bancarios convencionales, adquieren relevancia

cuando se combinan con canales de comunicación digital como redes sociales o páginas web.

En múltiples organizaciones islámicas radicadas en Europa, y particularmente en el Reino Unido, se ha documentado la existencia de secciones web dedicadas a donaciones, donde se proporcionan números telefónicos, correos electrónicos o direcciones físicas para establecer contacto y coordinar la transferencia del dinero. Estas donaciones, aunque formalizadas mediante métodos convencionales, son coordinadas a través de medios digitales que dificultan el rastreo institucional. Como señalan informes recientes, este método de contacto directo sigue vigente en muchas ONG islámicas vinculadas a mezquitas, madrazas o asociaciones humanitarias de fachada (Charity Commission for England and Wales, 2013; Charity Commission for England and Wales, 2015).

Un caso paradigmático es el de la ONG "Acción Internacional por los Refugiados Iraquíes" (IAFIR), cuyas cuentas de 2015 evidenciaron la recepción y entrega de fondos en efectivo por valor de miles de libras esterlinas. Esta práctica es posible en parte debido a la menor regulación de pagos en metálico existente en Reino Unido frente a países como España, lo que permite movimientos importantes de dinero sin obligación inmediata de justificar el origen o destino de los fondos.

Asimismo, existen herramientas tecnológicas adaptadas al contexto humanitario y que, sin embargo, pueden ser manipuladas para fines ilegítimos. Un ejemplo particularmente sofisticado es el sistema de tarjetas E-Aid desarrollado por la organización Al-Fatiha Global. Estas tarjetas electrónicas se distribuían entre familias sirias y turcas desplazadas, con PIN, instrucciones de uso y listado de productos subvencionables. Aunque la intención era dignificar la ayuda, su mal uso —como la reventa de artículos o connivencia con comerciantes afines— podía convertir el mecanismo en una fuente de desvío financiero sin supervisión efectiva (Al-Fatiha Global, 2017; Mancebo, 2018).

Finalmente, debe subrayarse el uso masivo y cada vez más perfeccionado del crowdfunding. Plataformas como Muslim Giving, GiveBrite, Just Giving o MyDonate permiten lanzar campañas sin necesidad de contar con un sitio web propio. Muchas de estas iniciativas han sido aprovechadas por entidades como One Nation UK o One Ummah, con amplia presencia en Siria y otros territorios de conflicto. En el caso de esta última, se han identificado campañas promovidas desde perfiles personales como el del condenado yihadista Yusuf Galán, en las que

se difundían imágenes de entregas de alimentos en Aleppo, acompañadas de enlaces a sitios de donación (CGPJ, 2020). Estos enlaces remitían, en ocasiones, a plataformas registradas antes de la legalización oficial de la propia ONG, lo que sugiere un uso fraudulento previo a su autorización por la Charity Commission británica (Mancebo, 2018).

La ambigüedad jurídica de estas plataformas, unida a la falta de supervisión externa en muchas campañas, ha sido señalada tanto por la Financial Action Task Force (FATF, 2023) como por la ONU (CTED, 2022), que denuncian el uso de “proyectos ficticios”, asociaciones fantasmas y campañas gestionadas por personas vinculadas con delitos de terrorismo

**VIII – ESTRATEGIAS DE
COMUNICACIÓN DIGITAL,
SEGMENTACIÓN
IDEOLÓGICA Y
CONSTRUCCIÓN DE LA
MARCA YIHADISTA**

VIII - ESTRATEGIAS DE COMUNICACIÓN DIGITAL, SEGMENTACIÓN IDEOLÓGICA Y CONSTRUCCIÓN DE LA MARCA YIHADISTA

8.1. MARKETING Y TERRORISMO: CONVERGENCIA DE IDEOLOGÍAS

El vínculo entre el marketing y el terrorismo puede parecer a primera vista una hipérbole analítica, sin embargo, la observación minuciosa de las prácticas propagandísticas de los grupos yihadistas revela la apropiación deliberada de lógicas comerciales y comunicativas propias del marketing contemporáneo. Esta hibridación entre dos esferas aparentemente inconexas tiene profundas implicaciones para el análisis criminológico, sociológico y comunicacional del terrorismo global.

La definición clásica de marketing formulada por Kotler y Armstrong (2003) lo describe como “un proceso social y administrativo por el que individuos y grupos obtienen lo que necesitan y desean a través de la creación y el intercambio de productos y de valor con otros” (p. 8). Bajo esta perspectiva, el marketing no se restringe a la transacción económica de bienes tangibles, sino que puede operar en el plano simbólico: productos ideológicos, narrativas, valores religiosos o marcos de interpretación del mundo también son susceptibles de ser “comercializados”, “posicionados” y “consumidos” por una audiencia.

Ya en la campaña presidencial de Eisenhower (1952), se observa un uso consciente de técnicas modernas de marketing político para moldear percepciones y ganar adhesión (Achache, 1992). Alonso (2000) enfatiza que todo proyecto que aspire a movilizar voluntades debe convencer al público, persuadir a través de imágenes, eslóganes, promesas y emociones. Este principio se aplica tanto a una marca comercial como a un movimiento insurgente. En efecto, como afirma Luna (2009), “el terrorismo es una guerra de marketing”.

En el contexto yihadista, esta dimensión se manifiesta con claridad. Daesh, en particular, ha sabido construir un “producto ideológico” potente: un califato islámico transnacional, con una promesa utópica de pureza religiosa, justicia social, comunidad redimida y vida plena bajo la sharía. Este producto se dirige a un

“mercado” compuesto por jóvenes musulmanes desencantados, radicalizados o en búsqueda de sentido existencial.

Aplicando la lógica del marketing mix (producto, precio, plaza, promoción), el califato se convierte en el “producto”; el “precio” es la renuncia a la vida pasada, incluso a la propia vida en misiones suicidas; la “plaza” son las redes sociales y foros donde se difunde el mensaje; y la “promoción” son las imágenes heroicas, los testimonios de mártires, los vídeos de ejecuciones editados con estética cinematográfica y las revistas como Dabiq o Rumiya.

En esta lógica de mercado simbólico, el consumidor no es pasivo: se convierte en actor dentro de una narrativa épica. Esta participación activa, emocional y totalizante distingue la comunicación terrorista de otras formas de propaganda clásica. No se trata solo de convencer, sino de reclutar, transformar y radicalizar.

La comunicación yihadista, por tanto, no es un fenómeno espontáneo sino fruto de una planificación estratégica consciente. El producto ideológico que ofrece Daesh se construye con técnicas de branding, storytelling y posición de mercado, adaptadas al lenguaje y los códigos de la audiencia joven globalizada. Como apunta Torres (2017), el mensaje no es accesorio al acto violento: “el mensaje es el acto terrorista”.

Esta convergencia entre terrorismo y marketing no debe banalizarse ni considerarse una mera estrategia propagandística. Se trata de un nuevo paradigma comunicacional, donde el terror deviene mensaje, el mensaje deviene marca, y la marca se expande como virus por los canales digitales del siglo XXI. Comprender esta fusión es imprescindible para diseñar contra narrativas eficaces y estrategias preventivas acordes a la era de la hiperconectividad.

8.2. SEGMENTACIÓN DEL PÚBLICO OBJETIVO YIHADISTA Y CONFIGURACIÓN DE MARCA

En el estudio de la propaganda yihadista contemporánea resulta crucial analizar el perfil sociodemográfico y psicológico de su audiencia destinataria. Lejos de lanzar sus mensajes de forma indiscriminada, las organizaciones terroristas como Daesh o Al Qaeda han perfeccionado estrategias de segmentación altamente eficaces, adaptadas a las condiciones de vulnerabilidad emocional y cultural de sus

receptores. En este contexto, los llamados millennials, jóvenes nacidos aproximadamente entre 1980 y 1996, que en el momento de eclosión del Califato islámico, tenían entre 16 y 30 años de edad, han ocupado un lugar central en las campañas de captación digital diseñadas por estos grupos. Su alta exposición tecnológica, el desencanto con las instituciones democráticas, la precariedad vital y la necesidad de pertenencia simbólica convierten a esta generación en una diana particularmente permeable al relato heroico y disruptivo del yihadismo global (Lesaca, 2017; Torres , 2016).

La atracción ejercida por Daesh sobre este grupo de personas se entiende mejor si se analiza desde el prisma de la teoría de la frustración-agresión desarrollada por Dollard y Miller en 1939, y reelaborada en contextos de violencia política por autores como Gurr (1970). Según esta perspectiva, las expectativas no cumplidas de reconocimiento, justicia o inserción social, especialmente en contextos de migración o marginación identitaria, alimentan una predisposición psicológica a buscar marcos de sentido alternativos. El relato del Califato islámico aparece entonces como una oferta existencial totalizadora que conecta a la perfección con el modelo 3N (Need, Narrative, Network): promete pertenencia, sentido, dignidad y trascendencia, todo ello revestido de una estética de rebelión y martirio que seduce precisamente por su radical alteridad respecto al mundo secular occidental, potenciando la predisposición a la violencia (Kruglanski et al, 2019).

Este fenómeno se acentúa en sociedades postindustriales donde el modelo de éxito se ha visto deslegitimado. Como advierte Bauman (2007), en las sociedades líquidas los individuos transitan entre vínculos efímeros y una permanente sensación de desarraigo. Los yihadistas han comprendido con aguda precisión esta crisis del sujeto contemporáneo, y han sabido dotar su mensaje de una épica que responde a la necesidad de identidad firme y de misión trascendente. En lugar del anonimato laboral y relacional que caracteriza a muchos jóvenes europeos, el Estado Islámico ofrece una causa sagrada, una comunidad fuerte, una promesa de honor y, para los más desesperanzados, la oportunidad de “redimirse” a través del sacrificio final.

Numerosos estudios de caso confirman esta dinámica. Es el caso paradigmático de Abdelhamid Abaaoud, cerebro de los atentados de París en 2015, nacido en Bélgica en el seno de una familia de origen marroquí. A pesar de contar con acceso a educación y recursos, su trayectoria vital estuvo marcada por el fracaso escolar, la delincuencia juvenil y el sentimiento de exclusión social (Suanzes, 2015). Fue precisamente a través de foros yihadistas y plataformas como Twitter y YouTube donde comenzó a construir su nueva identidad como “guerrero de la umma”, convencido de luchar por una causa superior. En sus comunicaciones, se dirigía a sus antiguos amigos del barrio no con odio, sino con una mezcla de paternalismo y desafío: “Vosotros perdéis el tiempo en fiestas, yo lucho por el Islam verdadero” (Mezzofiore, 2015).

Otro ejemplo representativo es el de Shamima Begum, ciudadana británica que, con apenas 15 años, abandonó Londres junto a otras dos adolescentes para unirse al Califato en Siria. Educada en un entorno occidental, sin antecedentes de marginalidad extrema, Begum fue captada por la narrativa de empoderamiento y purificación que circulaba en canales cerrados de Telegram, donde se presentaba la vida bajo la sharía como un retorno a la dignidad islámica perdida. Según declaró en entrevistas posteriores, el factor determinante no fue la violencia, sino “la promesa de hacer algo importante, de pertenecer a algo que valiera la pena” (Callimachi, 2019).

Este tipo de procesos reflejan un patrón común: la radicalización no se produce exclusivamente por adoctrinamiento teológico, sino como respuesta a una necesidad emocional y simbólica que no encuentra satisfacción en las estructuras tradicionales. Como señala Lesaca (2017), la propaganda yihadista construye una narrativa de redención mediante el sacrificio: “el joven frustrado, invisible para su entorno, puede convertirse en héroe global si abraza la causa del Califato”. Esta estrategia combina técnicas de marketing político, psicología de masas y religiosidad radicalizada en un producto ideológico altamente seductor.

En suma, el segmento “millennial” no solo es objetivo de la propaganda yihadista por razones tecnológicas (uso intensivo de redes, familiaridad digital), sino sobre todo por su disposición emocional y sociocultural a asumir relatos alternativos de sentido. Las campañas de Daesh lo entienden con precisión quirúrgica: se adaptan a sus códigos estéticos, sus frustraciones colectivas, su

imaginario audiovisual y su deseo de protagonismo. La captación no se produce desde la promesa de odio, sino desde la necesidad de pertenencia.

Una de las claves del éxito comunicativo de Daesh y otras organizaciones afines reside en su uso sofisticado del lenguaje audiovisual, directamente alineado con los hábitos de consumo cultural de los jóvenes de la era digital. En este contexto, las imágenes, los vídeos en alta resolución, las tipografías potentes, las melodías épicas y los efectos cinematográficos han desplazado a la doctrina como principal vehículo de atracción ideológica. Según Torres (2017), “la estética ha sustituido a la teología en el proceso de radicalización”, una afirmación que cobra especial relevancia al analizar las revistas Dabiq y Rumiya, producidas en múltiples idiomas y adaptadas para diferentes públicos.

Estas publicaciones no solo informan sobre atentados, sino que articulan una cosmovisión heroica, identitaria y escatológica. El contenido se estructura en torno a tres pilares:

1. *La denuncia de la humillación del islam a manos de Occidente*: La ideología yihadista parte de una lectura victimista de la historia islámica contemporánea, en la que el islam aparece como civilización oprimida y humillada por siglos de colonialismo, intervenciones militares y decadencia moral promovida por Occidente. Como señala Kepel (2004), esta percepción construye una “mitología del agravio”, en la que el islam debe defenderse frente a un mundo hostil que lo degrada y persigue.
2. *La exaltación de la umma como cuerpo global redentor*: La propaganda de Daesh y Al Qaeda promueve una visión unificada de la umma como comunidad trascendente que debe restaurar su dignidad mediante el retorno al Califato y la aplicación de la sharía. Según Awan (2017), esta narrativa ofrece a los jóvenes marginados “un sentimiento de pertenencia a una comunidad heroica que trasciende fronteras y otorga sentido a sus vidas”.
3. *La glorificación del mártir como agente de justicia divina*: La figura del mártir ocupa un lugar central en la iconografía yihadista, presentada no como víctima sino como ejecutor de una justicia superior. Como indica Winter

(2015), la propaganda visual del Estado Islámico eleva al shahid a un plano casi mítico, mostrándolo como “el héroe que restaura el equilibrio cósmico roto por la injusticia de los infieles”.

Esta narrativa opera como una inversión de los relatos tradicionales de éxito occidental, donde el joven frustrado, relegado o disidente se convierte en protagonista universal de un drama sagrado. En este sentido, autores como Sageman (2004), exanalista de la CIA y psiquiatra, han subrayado que la mayoría de los yihadistas occidentales no eran “locos religiosos, sino jóvenes en busca de identidad, reconocimiento y propósito”.

Es este deseo de significación lo que explica el poder de la “narrativa épica” que subyace a la propaganda yihadista. Lesaca (2017) afirma que la comunicación de Daesh se estructura como un guion de ficción heroica: el protagonista (el joven musulmán) se enfrenta a una injusticia global (la persecución del islam), encuentra una comunidad que le ofrece sentido (la umma radical) y alcanza la redención a través de la lucha (la yihad armada). Este modelo responde fielmente al esquema del viaje del héroe clásico identificado por Campbell (2001), trasladado ahora a un escenario de guerra espiritual digitalizada.

La selección de plataformas también responde a criterios de segmentación. Twitter, Instagram, Telegram, YouTube o TikTok no se utilizan de manera aleatoria, sino según los hábitos demográficos de cada franja de edad. En el caso de los más jóvenes, los mensajes se adaptan con memes, música de moda, formatos breves y subtítulos, mientras que para públicos más maduros se ofrece contenido ideológico de mayor densidad. Esta estrategia, según Khatib (2014), permite a los yihadistas “colonizar espacios comunicativos” donde tradicionalmente solo circulaban mensajes comerciales o de ocio.

Un ejemplo notable de esta flexibilidad fue el de Junaid Hussain, ciudadano británico de origen paquistaní y hacker afiliado a Daesh, conocido por su intensa actividad digital. Según (Hamid, 2018), Hussain gestionaba cuentas de Twitter que combinaban memes, amenazas, versos coránicos y videos de asesinatos con música de rap, lo que le permitió atraer una audiencia joven y tecnófila. Antes de morir en un ataque con drones en Siria en 2015, había acumulado decenas de miles de seguidores y figuraba en la lista de objetivos prioritarios del Pentágono (NPR, 2015). Su perfil combinaba la rebeldía pop, la tecnofilia hacker y el radicalismo teológico en una mezcla diseñada para atraer a jóvenes alienados.

Esta conexión emocional con la audiencia también se refuerza con la idea de “comunidad virtual” o hermandad simbólica. Las redes sociales permiten a los aspirantes conversar directamente con otros reclutas, recibir aprobación simbólica por sus ideas, y formar parte de un microcosmos donde el islam salafista-yihadista es la norma. Tal como señala Neumann (2016), “el proceso de radicalización muchas veces se asemeja más a una conversión afectiva que a un adoctrinamiento dogmático”, lo que refuerza la importancia de los vínculos interpersonales digitales en el proceso.

Este fenómeno ha sido especialmente visible en casos como el de Hayat Boumeddiene, pareja de Amedy Coulibaly, uno de los autores de los atentados de París en 2015. Hayat no participó directamente en los ataques, pero fue radicalizada mediante redes sociales y foros salafistas donde halló un entorno de validación emocional que no había encontrado en su entorno social o familiar. Tras los atentados, huyó a Siria y se convirtió en icono del islamismo radical femenino, apareciendo incluso en fotografías armada y sonriente junto a combatientes. Su perfil demuestra que la propaganda yihadista sabe adaptar sus códigos para atraer también a mujeres jóvenes, presentándoles un relato de empoderamiento religioso y de ruptura con la opresión secular (Vidino & Hughes, 2015).

Esta es la verdadera potencia del marketing yihadista: no se limita a informar, sino que seduce, emociona, apela al deseo profundo de trascendencia y pertenencia. La segmentación del público no es solo una cuestión demográfica, sino fundamentalmente psicológica y afectiva.

Otro aspecto de la propaganda yihadista, es la esfera destinada a la captación de conversos o incluso individuos sin vínculos culturales profundos con el islam, que en virtud de la barrera que supone el desconocimiento de la lengua árabe, y por tanto la incapacidad de comprender los sermones de las mezquitas, ha facultado que Internet se erija como el pedestal de su adoctrinamiento y elemento para canalizar su frustración (Baquero, 2008). Esta frustración no es exclusivamente económica o social, sino que muchas veces es identitaria y existencial. La narrativa yihadista no vende simplemente violencia, vende un lugar en el mundo, una causa por la cual vivir y morir, y una comunidad de sentido que sustituye a un entorno que los ha rechazado, marginado o invisibilizado.

Diversos autores han abordado esta dimensión desde una perspectiva generacional. El politólogo Reinares (2017) afirma que “la mayoría de los yihadistas europeos eran jóvenes integrados en apariencia, pero desvinculados emocionalmente del sistema liberal que los acogía, con una biografía marcada por el desencanto, el aislamiento o la experiencia carcelaria”. No es casual que muchos procesos de radicalización comiencen en prisiones, donde la identidad islámica sirve de escudo frente a la humillación, y el adoctrinamiento encuentra terreno fértil en el resentimiento.

Este sentimiento de exclusión ha sido identificado también por Rieff (2016), quien advierte que “en muchos casos no se trata de un odio al estilo de vida occidental, sino del dolor de no sentirse parte de él”. Aquí es donde el yihadismo logra invertir el guion, pues no hay que luchar por integrarse, sino reivindicar con orgullo la diferencia. La estética del rechazo, del orgullo salafista, de la superioridad moral frente al hedonismo de Occidente, seduce a jóvenes desencantados que encuentran en el islamismo radical una forma de rebeldía que justifica su ira.

El perfil de Abdelhamid Abaaoud ilustra esta lógica. De origen marroquí, nacido en Bélgica, pasó de ser un delincuente común en los suburbios de Bruselas a convertirse en el cerebro de los atentados de París en 2015. Su paso por prisión fue determinante en su proceso de radicalización. Una vez en Siria, posó en vídeos de propaganda, se burló de la policía belga y fue presentado como modelo de héroe yihadista por las revistas de Daesh. Abaaoud se convirtió en símbolo del “renacido” que, tras una vida de crimen y vacío, encuentra redención en la guerra santa. Su caso fue ampliamente difundido en medios sociales, no solo como propaganda, sino como ejemplo a seguir.

Otro ejemplo paradigmático es el de Mehdi Nemmouche, autor del atentado en el Museo Judío de Bruselas en 2014. Francés de origen argelino, también se radicalizó en prisión. A su regreso de Siria, donde combatió con Daesh, actuó en solitario, lo que lo convierte en uno de los primeros “retornados” activos en Europa. Lo más preocupante del caso Nemmouche es que su acción no fue ordenada por una cúpula, sino inspirada por una ideología difusa pero potente, difundida digitalmente, y asumida como propia. Como ha señalado el Centro de Análisis del Terrorismo Francés (CAT), “el 60 % de los atacantes yihadistas

recientes en Europa actuaron sin vínculo operativo directo, pero con plena fidelidad simbólica a Daesh”.

En esta línea, el fenómeno de los “lobos solitarios” debe entenderse como una consecuencia directa del modelo de propaganda segmentada. No se trata de individuos locos, sino de sujetos captados por una narrativa que les permite actuar por su cuenta sin necesidad de instrucciones formales. La identidad digital y la fidelidad ideológica suplen la pertenencia orgánica. Daesh ha sabido cultivar ese modelo, otorgando el título de “mártir del califato” a cualquier atacante que justifique su acto en nombre del islam o jurando fidelidad manifiesta a la organización terrorista y se grabe o difunda el mensaje.

La estrategia se completa con la construcción de una marca identitaria coherente, basada en valores simples pero potentes: dignidad, venganza, justicia, pureza, honor, hermandad. Estos valores son presentados como contracultura frente a la banalidad, corrupción y decadencia del mundo moderno. Así, el yihadismo se convierte en una oferta integral: da sentido, da identidad, da comunidad y da acción. La violencia no es el fin, sino el medio para cumplir esa promesa de redención.

Desde una perspectiva de marketing político, podríamos afirmar que Daesh ha sido una de las organizaciones más eficaces del siglo XXI en cuanto a construcción de marca, fidelización de clientes y segmentación de mercado. La elección de hashtags, los memes, los vídeos adaptados por idiomas, los testimonios de mártires, los eslóganes breves (“Ven a la tierra del califato”, “Muere con honor”, “Defiende al profeta”), todo obedece a una lógica de consumo simbólico intensivo. Esta lógica, como explica Luna (2009), “utiliza la emoción como vector de lealtad”, y en un entorno tan saturado de mensajes como Internet, lo emocional prima sobre lo racional.

Por ello, la lucha contra la propaganda yihadista no puede limitarse a censurar contenidos o cerrar perfiles, debe comprender su atractivo emocional y simbólico, desmontar sus promesas, y ofrecer contranarrativas igualmente sólidas y seductoras. Como advierte el profesor Neumann (2016), “el vacío no lo llena la represión, lo llena un relato mejor”.

8.3. NARRATIVA TRANSMEDIA Y ESTRATEGIA PROPAGANDÍSTICA

8.3.1. **Convergencia de formatos en la dimensión multimedia del relato yihadista**

Desde el inicio de su proyección internacional, Daesh comprendió que no bastaba con aterrorizar mediante la violencia física transmitida a través de innumerables formas como ejecuciones, decapitaciones, ahogamientos, prendimientos, crucifixiones, etc. Si no que, fueron plenamente conscientes del potencial asociado a la violencia simbólica, un tipo de violencia ejercida a través de una sofisticada arquitectura propagandística, que se convirtió en una de sus armas más poderosas. El uso convergente de formatos como el video, la infografía, los *nasheeds* (cánticos religiosos vestidos de heroicidad yihadista), los comunicados de prensa y las revistas digitales en distintos idiomas, permitió construir un ecosistema propagandístico total. Este no solo difundía el mensaje, sino que lo moldeaba, amplificaba y dotaba de un aura de legitimidad para audiencias diversas.

Una de las claves de esta estrategia radicó en la profesionalización de su aparato mediático. A diferencia de Al Qaeda, más rudimentaria en sus medios y narrativa, el autodenominado Estado Islámico desplegó una estética visual altamente cuidada. Los vídeos, como los difundidos por Al Hayat Media Center, destacan por su calidad cinematográfica, guiones dramáticos y montaje dinámico, recurriendo a cámaras lentas, música épica y subtítulos multilingües (Lesaca, 2017). Ejemplos emblemáticos como el vídeo del piloto jordano Muath al-Kasasbeh quemado vivo o las ejecuciones masivas en la playa de Libia ante cristianos coptos, no solo muestran el acto criminal, sino que lo envuelven en una narrativa simbólica destinada a provocar horror en el enemigo y admiración en el simpatizante.

A ello se suman las infografías producidas por agencias como Al Amaq y Al Naba, que ofrecen resúmenes visuales de los “logros” militares de la organización. Estas gráficas, casi siempre con tipografía árabe caligráfica, fondos oscuros y un lenguaje triunfalista, simulan los informes de los Estados modernos, con cifras, mapas, y estadísticas que buscan conferir verosimilitud a sus afirmaciones. Una de ellas, publicada tras los atentados en Cataluña de 2017, enumeraba las acciones

armadas en Europa, presentando la masacre como parte de una estrategia bélica racional y calculada (Europa Press, 2017).

En paralelo, la dimensión auditiva adquirió una relevancia insoslayable. Los llamados *anasheed* o cánticos religiosos guerreros, son empleados como banda sonora de sus producciones audiovisuales. Estas melodías, con letras en árabe clásico, ensalzan el martirio, el sacrificio y la lucha contra los infieles, actuando como medio de cohesión identitaria y emocional. En producciones como las de Ajnad Media Foundation, el mártir es retratado como un héroe eterno cuya sangre fertiliza el camino del Califato (MEMRI, 2022).

Las revistas digitales como Dabiq y Rumiyah representan otro pilar fundamental del aparato propagandístico. Redactadas en múltiples lenguas (inglés, francés, alemán, turco, entre otras), estas publicaciones combinan artículos doctrinales, entrevistas a combatientes y secciones operativas dirigidas a “lobos solitarios” en Occidente. En el número 5 de Rumiyah, por ejemplo, se ofrece una guía detallada para perpetrar atentados con cuchillos o vehículos, justificando su legitimidad mediante interpretaciones sesgadas del Corán y de la jurisprudencia islámica clásica (Dabiq, 2016).

En el plano de las redes sociales, el Daesh ha demostrado un conocimiento táctico de las plataformas. Durante sus años de auge (2014–2017), llegó a tener más de 46.000 cuentas activas solo en Twitter, muchas de ellas controladas por bots o cuentas coordinadas para amplificar mensajes (Berger & Morgan, 2015). Esta ocupación estratégica del ciberespacio no era caótica, sino profundamente estructurada, con funciones diferenciadas, unas cuentas se dedicaban a difundir comunicados; otras, a reclutar; algunas, a interactuar emocionalmente con posibles candidatos a la radicalización.

Así pues, no nos encontramos ante un uso incidental o espontáneo de diversos formatos, sino ante una estrategia meticulosamente orquestada de convergencia mediática. La eficacia de esta estrategia no se mide únicamente en visualizaciones o compartidos, sino en su capacidad para moldear percepciones, alentar acciones y mantener cohesionadas a comunidades extremistas dispersas por el mundo. Como ha señalado Torres (2017), “la propaganda yihadista es tanto una herramienta de guerra como de gobernanza simbólica”.

8.3.2. De la doctrina al espectáculo propagandístico en el relato transmedia

Tal y como hemos ido desarrollando a lo largo de este capítulo, la narrativa yihadista de Daesh no solo emplea múltiples formatos de forma simultánea, sino que los articula siguiendo una lógica que responde con precisión al modelo del transmedia storytelling, conceptualizado por Jenkins (2011). Según este autor, el relato transmedia se construye cuando los elementos de una historia se distribuyen de forma coordinada a través de distintos canales y medios, permitiendo que cada uno contribuya de manera singular a la experiencia del público. No se trata de redundancia, sino de expansión, cada formato añade una nueva capa de significado, generando una experiencia inmersiva.

Daesh, en este sentido, no ha desarrollado una narrativa: ha creado un universo simbólico total, una mitología moderna con héroes, enemigos, lugares sagrados, normas de vida y rituales de paso. La proclamación del Califato en 2014 se presentó como el renacimiento de la edad dorada islámica; un hito que no solo tenía dimensión política y religiosa, sino también estética y emocional. Desde ese momento, cada contenido mediático contribuyó a reforzar ese imaginario.

Así, mientras los vídeos muestran las victorias en combate, las ejecuciones y la vida cotidiana en las zonas controladas por el Califato, las revistas como Dabiq o Rumiyaah aportan el sustento doctrinal, el análisis geopolítico y los argumentos jurídicos. Las infografías, por su parte, simplifican los éxitos militares o las estadísticas de atentados para un consumo rápido y viral; y los nasheed ofrecen el marco emocional y espiritual. Incluso los memes difundidos en plataformas como Telegram o Rocket.Chat cumplen una función simbólica, ironizan sobre la debilidad de los enemigos y alimentan la épica de la resistencia (Torres , 2017).

Un ejemplo de esta narrativa transmedia lo hallamos en el tratamiento de las ejecuciones de rehenes occidentales. En el caso del periodista James Foley, asesinado en 2014, el aparato de propaganda difundió, de forma sincronizada, un vídeo de la ejecución, un comunicado en formato texto, un mensaje visual para redes sociales con frases coránicas (The Wall Street Journal, 2014), y un artículo en Dabiq justificando teológicamente el acto. El objetivo era múltiple: atemorizar,

explicar, adoctrinar y reclutar. Cada pieza era distinta, pero todas encajaban en un mismo relato global.

Otro ejemplo paradigmático es la difusión de atentados como el del Bataclan en París (2015). A través del hashtag #Paris_On_Fire, los canales yihadistas en redes sociales compartieron imágenes del ataque, felicitaciones a los autores, memes con la Torre Eiffel en llamas, y vídeos con montajes musicales que combinaban declaraciones del portavoz de Daesh con escenas del atentado. En paralelo, Rumiyah publicó una crónica del atentado con exaltación teológica de los suicidas, y en Telegram circularon guías para reproducir acciones similares en otras capitales europeas (Lesaca, 2017).

La lógica transmedia también permite la segmentación de audiencias, adaptando el mensaje a diferentes contextos culturales y lingüísticos. Por ello, Daesh editó publicaciones como *Dar al islam* en francés, *Konstantiniyye* en turco, *Istok* en ruso, o *Al-Risalah* en inglés. Cada una de estas revistas ofrece contenidos similares, pero con matices locales. La *Dar al islam*, por ejemplo, dedica secciones específicas a la comunidad musulmana francófona, mientras que *Istok* articula la narrativa desde la perspectiva del conflicto en el Cáucaso y Asia Central (Jihadology, 2016).

En este sentido, Daesh adopta el principio empresarial de franquiciar el relato, no impone un único mensaje, sino que ofrece una base común susceptible de adaptarse a contextos distintos, siempre y cuando se mantenga la fidelidad a la narrativa fundacional del Califato. Esta flexibilidad explica, en parte, su éxito en la captación de individuos de más de 100 nacionalidades, con perfiles muy diversos, desde adolescentes sin arraigo social hasta profesionales con estudios superiores.

La eficacia de esta estrategia no reside únicamente en la calidad técnica de los productos, sino en su coherencia simbólica. Cada pieza propagandística, por más pequeña que sea, remite a un universo mayor, donde todo tiene sentido, el mártir no muere sino que asciende al paraíso; los enemigos del islam mueren fortaleciendo la fe de la umma; la vida bajo el Califato es dura, pero justa; Occidente es corrupto y decadente; el musulmán indignado tiene un deber que cumplir. No se trata de persuadir, sino de convocar a una comunidad global en guerra.

8.3.3. Las fábricas del relato: Al Hayat, Al Furqan, Al Amaq y las Willayat mediáticas del Califato

La narrativa transmedia del Daesh no habría alcanzado su dimensión expansiva sin la existencia de una infraestructura mediática compleja y especializada, diseñada con lógica industrial y jerarquía funcional. A partir de 2014, con la proclamación del Califato, el grupo terrorista invirtió sistemáticamente en la creación de centros de producción de contenidos que cubrieran no solo el frente bélico, sino también el cultural, religioso y propagandístico. Entre ellos destacan Al Hayat Media Center, Al Furqan Foundation y Al Amaq News Agency, pilares fundamentales del relato yihadista global.

Al Hayat Media Center fue concebido como la plataforma principal de proyección internacional del Califato. Sus productos están dirigidos a una audiencia occidental o multilingüe, con materiales editados en inglés, alemán, francés, español, ruso o turco. En sus vídeos se observa una deliberada estética hollywoodense, con narrativas estructuradas, planos cuidados y efectos sonoros que generan una atmósfera de épica heroica. Uno de los vídeos más conocidos fue *Flames of War*, una especie de documental bélico que presenta las batallas del Daesh como una cruzada contra la corrupción de Occidente y sus aliados. En él, combatientes angloparlantes actúan como narradores de la historia, dirigiéndose directamente al espectador musulmán europeo para que “despierte” y se una a la lucha (Al Hayat, 2014).

Al Furqan Media Foundation, por su parte, es el órgano responsable de los comunicados oficiales, discursos de los líderes y declaraciones doctrinales. Su tono es más sobrio, con un enfoque institucional. A través de esta plataforma se difundieron los célebres mensajes de Abu Bakr al-Baghdadi, entre ellos su primer discurso como califa en la mezquita de Al-Nuri en Mosul en el 2014, que fue filmado desde varios ángulos y subtulado en múltiples idiomas. Al Furqan también es conocida por lanzar los vídeos más impactantes de ejecuciones y torturas, dotándolos de una estética siniestra pero cuidada, donde el horror se transforma en espectáculo mediático.

Al Amaq News Agency, en cambio, funciona como agencia semioficial de noticias. Fundada en 2014, comenzó como una plataforma en Telegram pero rápidamente diversificó sus canales. Amaq se presenta como un medio informativo

objetivo, que “cubre” los avances del Daesh en Siria, Irak, África o Asia Central. En cada atentado perpetrado por la organización o sus filiales, Amaq emite breves comunicados reivindicativos, acompañados de imágenes, infografías o vídeos. Esta estrategia permite a Daesh apropiarse del lenguaje de la prensa contemporánea, generando confusión entre propaganda y periodismo. Su canal en Telegram, durante los años de máximo apogeo, alcanzó más de 20.000 suscriptores (MEMRI, 2020).

Junto a estas productoras centrales, Daesh fomentó la descentralización mediante la creación de wilayat mediáticas, pequeñas delegaciones propagandísticas asignadas a cada región bajo control o influencia. Así surgieron en Siria: *Wilayat Al-Raqqa* en la capital administrativa del Califato; *Wilayat Al-Barakah* en la provincia de Al-Hasaka; *Wilayat Al-Khayr* en la región de Deir ez-Zor; *Wilayat Homs* en las zonas rurales de Homs; *Wilayat Dimasqh* en la zona sur y la periferia del país; *Wilayat Halab* en la zona de Aleppo; *Wilayat Al-Badiyah* en la zona desértica central (Lister, 2015). Y de igual forma, en otras regiones en las que la organización ha ido copándose de influencia: *Wilayat Khurasan* (Afganistán-Pakistán), *Wilayat al-Barqah* (Libia), *Wilayat Gharb Ifriqiyyah* (Nigeria), *Wilayat Sinai* (Egipto), entre otras. Cada una de ellas con capacidad de generar contenidos propios, adaptados al entorno local, en lenguas autóctonas, con protagonistas regionales, pero manteniendo el estilo visual y el marco ideológico común del Califato. Esta fórmula permitía mantener la cohesión doctrinal al tiempo que se aseguraba la proximidad cultural con los simpatizantes locales.

En Libia, por ejemplo, los vídeos de *Wilayat Tarabulus* mostraban patrullas religiosas, castigos públicos y distribución de pan, con una narrativa centrada en la restauración de la justicia islámica. En el Sahel, los vídeos de *Wilayat Gharb Ifriqiyyah* combinaban ataques contra el ejército nigeriano con imágenes de campamentos de entrenamiento y juramentos de lealtad a al-Baghdadi por parte de jóvenes locales. En todos los casos, el formato imitaba las pautas marcadas por Al Hayat y Al Furqan, generando una estandarización visual y semiótica.

Este sistema jerárquico distribuido a través de productoras centrales para difusión global, y wilayat para enfoque local, replicaba la lógica estatal: un Ministerio de Información descentralizado pero ideológicamente cohesionado, que

garantizaba la difusión permanente de una narrativa épica, apocalíptica y polarizadora. En palabras de Lesaca (2017) el aparato de comunicación del Daesh fue estructurado con una precisión “propia de una maquinaria de guerra propagandística”, donde cada unidad sabía qué mensaje producir, a qué público dirigirse y por qué canal distribuirlo.

8.3.4. Las revistas y su modulación ideológica del mensaje yihadista

Uno de los aspectos más sofisticados de la maquinaria propagandística del Estado Islámico residía en su capacidad para fragmentar su discurso ideológico sin perder cohesión doctrinal, adaptando mensajes, formatos y lenguas según el perfil del receptor. Esta estrategia no solo permitió optimizar la captación de nuevos miembros, sino también articular una comunidad simbólica transnacional. Como señala Lesaca (2017), la organización implementó un modelo de comunicación glocal: “global en su ambición, pero local en su ejecución discursiva” (p. 115).

Las revistas *Dabiq*, *Rumiyah*, *Dar al-Islam*, *Konstantiniyye* o *Istok* no son simples boletines doctrinales. Cada una fue concebida como vehículo de adoctrinamiento adaptado al contexto cultural, lingüístico y político del lector objetivo. Así, *Dabiq*, editada en inglés, apelaba a los occidentales conversos o a musulmanes de segunda generación criados en Europa o Estados Unidos. Se caracterizaba por un lenguaje pulido, referencias históricas cuidadosamente seleccionadas y una cuidada estética visual que emulaba las revistas de análisis político-militar occidental (Callimachi, 2015).

En contraste, *Dar al-Islam* dirigida al público francófono intensificaba el tono combativo y victimista, buscando movilizar a jóvenes musulmanes marginados en las periferias urbanas de Francia o Bélgica. Utilizaba un lenguaje más emocional, con apelaciones directas al sentimiento de humillación identitaria y a la urgencia de “vengar” las supuestas afrentas a la *umma* en Siria, Palestina o Afganistán. Como subraya Reinales (2018), esta publicación fue particularmente eficaz tras los atentados de París y Niza, cuando logró canalizar el resentimiento social hacia una forma de activismo violento (p. 88).

Otro ejemplo de esta narrativa segmentada fue *Konstantiniyye*, redactada en turco y centrada en atacar al gobierno secular de Turquía, al que acusaba de

traicionar los principios del islam y de colaborar con “los cruzados” (Yayla & Speckhard, 2017). En Rusia, Istok se dirigía al Cáucaso y a los musulmanes del Asia Central, ofreciendo una reinterpretación heroica del legado de Shamil Basayev y otros líderes de la insurgencia chechena. En todos los casos, la estrategia consistía en insertar el relato yihadista dentro del marco simbólico del entorno del lector (Torres, 2020, p. 156).

La selección de los nombres de estas publicaciones tampoco fue arbitraria. Dabiq alude a una localidad en Siria donde, según una profecía islámica recogida por Abu Hurayrah, se librará la batalla final entre musulmanes y cruzados (Warrick, 2015). Rumiya, sucesora de Dabiq, significa “Roma” en árabe y remite directamente a Occidente como objetivo último de la conquista simbólica. Como apunta Callimachi (2017), el paso de Dabiq a Rumiya no fue solo semántico, sino estratégico pues la caída de la ciudad homónima obligó a Daesh a renovar su imaginario apocalíptico para mantener la moral de sus simpatizantes.

El caso de las revistas Al-Naba, Sawt al-Hind o Al-Balagh, surgidas tras la caída del califato territorial, continúa esta lógica. Al-Naba, publicada de forma semanal en árabe, actúa como boletín oficial del grupo y sirve para coordinar narrativas entre las distintas wilayat (MEMRI, 2021). Sawt al-Hind, editada en inglés por el grupo afín al Estado Islámico en el subcontinente indio (ISHP), está claramente dirigida a jóvenes radicalizados de India, Bangladesh y Pakistán. Al-Balagh, por su parte, surge del entorno del Estado Islámico de Khorasan (ISIS-K), que ha tomado el relevo comunicacional tras el colapso físico del califato sirio-iraquí (Counter Extremism Project, 2023).

Cabe destacar que esta fragmentación geográfica y cultural del mensaje no implica disonancia en los objetivos: todos los canales responden a un marco doctrinal común y a una estrategia meta comunicativa unificada. De hecho, la continuidad editorial y la repetición de ciertos motivos —la nostalgia por el califato, el martirio como exaltación, el enemigo común “cruzado y sionista” — aseguran una identidad compartida que trasciende los idiomas y las fronteras (Vidino, 2015).

Así, el proyecto comunicativo del Daesh no fue improvisado ni meramente táctico, sino un instrumento de gobernanza simbólica orientado a modelar identidades, justificar la violencia y perpetuar una cosmovisión teocrática. Esta

capacidad de sincronizar múltiples narrativas hacia un mismo horizonte ideológico convirtió al aparato mediático del Daesh en un actor con autonomía estratégica propia (Torres, 2020, p. 163).

8.3.5. Análisis crítico del impacto de la propaganda yihadista

El éxito del aparato propagandístico del Estado Islámico no puede medirse únicamente por la calidad de sus productos comunicativos, sino que debe ser medido por su capacidad de inspirar conductas extremas, movilizar combatientes y multiplicar la violencia a escala global. Las narrativas de Daesh eran meros ejercicios retóricos; constituían dispositivos estratégicos de reclutamiento, cohesión ideológica y activación operativa. Como advierte el politólogo Ingram (2017), “el poder de la propaganda del Estado Islámico reside en su equilibrio entre lo empírico y lo emocional, entre la utopía teológica y el horror performativo” (p. 1).

El caso del atentado de Manchester (2017), en el que el joven Salman Abedi detonó un artefacto explosivo en un concierto de Ariana Grande, es paradigmático. Abedi había sido expuesto durante años a la propaganda de Daesh, incluyendo los vídeos de Al Hayat y discursos de Anwar al-Awlaki, reutilizados por los canales oficiales del grupo. Investigaciones policiales confirmaron que el atacante se había radicalizado mediante contenido online, sin haber viajado a Siria ni haber recibido entrenamiento físico, lo que evidencia el poder autoradicalizador y formador del ecosistema digital yihadista (BBC News, 2017).

Otro caso inquietante es el del tunecino Mohamed Lahouaiej-Bouhlel, quien en julio de 2016 perpetró un atropello masivo en Niza que dejó 86 muertos. Aunque inicialmente no constaban vínculos directos con Daesh, días después la organización asumió su autoría a través de Al Amaq. El análisis forense de sus dispositivos reveló búsquedas intensivas de vídeos de ejecuciones, discursos del Daesh y contenido gráfico glorificando la violencia de los mártires (Reinares, 2018). La propaganda había funcionado como catalizador psicológico y radicalizador, proporcionando justificación, modelo de acción y ritual de paso.

Un elemento especialmente eficaz de la estrategia comunicativa de Daesh fue su habilidad para fusionar medios visuales y narrativas épicas. En el caso del atentado de Bataclan (París, 2015), la campaña de difusión en redes sociales incluyó

imágenes con hashtags como #ParisOnFire o #FranceUnderAttack, anticipando la ola de viralización antes incluso de que los cuerpos fueran retirados del teatro. Como documentó Lesaca (2017), los yihadistas activaron más de 2.000 cuentas en pocas horas, muchas con mensajes coordinados en inglés, francés, árabe y turco. Esta maniobra convirtió el atentado en un evento transnacional, reforzando el aura de omnipresencia de Daesh.

En otro plano, la revista Rumiya, que sucedió a Dabiq tras la pérdida del territorio sirio bajo su nombre, se centró en guiar atentados individuales en Occidente. En el número 2, por ejemplo, se detallaba cómo emplear un camión para maximizar las víctimas en un mercado navideño, anticipando así lo que más tarde sería el ataque en Berlín (2016), perpetrado por Anis Amri. Este tipo de contenidos no solo instruyen, sino que transforman a los simpatizantes en “lobos” instruidos en la operativa táctico-militar. De ahí que muchos expertos, como Vidino (2015), hablen ya no de propaganda sino de “tutorial de guerrilla urbana”.

La efectividad de la narrativa yihadista también se evidencia en el plano emocional. Varios reclutas entrevistados por investigadores de la Universidad George Washington señalaron que los vídeos de Daesh les ofrecían algo que no encontraban en sus entornos cotidianos: sentido, pertenencia y trascendencia. La imagen del mártir —joven, digno, sonriente antes de inmolarse— se contrapone al estigma social del joven musulmán alienado en Occidente. Como explica Speckhard (2020) “el martirio se convierte en una forma de redención simbólica frente a la humillación y la banalidad vital”.

Ahora bien, esta maquinaria propagandística no está exenta de contradicciones ni de puntos débiles. La sobreexposición de la violencia, los relatos hiperbólicos y el culto a la crueldad extrema generaron una reacción de rechazo incluso en círculos yihadistas más tradicionales. Al Qaeda, por ejemplo, criticó duramente a Daesh por “perder el control estratégico del mensaje”, acusándolo de anteponer el impacto mediático a la prudencia ideológica (MEMRI, 2015). Este debate, lejos de ser marginal, refleja el conflicto entre visibilidad y viabilidad en el seno del yihadismo global.

Otro límite significativo fue la dependencia de plataformas convencionales. Tras la presión ejercida por gobiernos y empresas tecnológicas entre 2016 y 2020,

Twitter, YouTube y Facebook cerraron decenas de miles de cuentas vinculadas al Daesh. Esto forzó un desplazamiento hacia redes más opacas como Telegram, Rocket.Chat o JustPaste.it, reduciendo la capacidad de penetración en audiencias no radicalizadas. La propaganda sobrevivió, pero perdió parte de su efecto de contagio masivo.

En síntesis, ante todo lo expuesto en este capítulo, el Estado Islámico logró construir una máquina propagandística sin precedentes en el universo del terrorismo contemporáneo. Mediante técnicas de marketing, storytelling apocalíptico y un dominio semiótico del espacio digital, convirtió cada ataque en una campaña publicitaria, cada mártir en un emblema y cada víctima en parte del relato. Su eficacia no radicó solo en lo que decía, sino en cómo lo decía, a quién se dirigía, con qué ritmo y en qué soporte. Sin embargo, su exceso estético y doctrinal, sumado a la pérdida de su base territorial con la caída de sus últimos bastiones, Deir ez-Zor a finales del 2017, y Baghouz en 2019 facultaron en gran medida la erosión de la galaxia mediática yihadista. Sin embargo, para nada se puede hablar de su derrota mediática, pues su herencia propagandística ha sido retomada y adaptada hoy en día por actores como Daesh Khorasan (ISIS-K) o Al-Malahem Media.

8.3.6. La herencia del relato tras la caída del Califato islámico de Daesh

La derrota territorial del Estado Islámico en Siria e Irak, culminada simbólicamente con la caída de Baghouz en 2019, no supuso la extinción de su aparato mediático, sino más bien su mutación y descentralización. Si en su apogeo Daesh operaba como un “ministerio de propaganda” centralizado con capacidad de producción profesional (Al Hayat, Al Furqan, Al Amaq), su descomposición estructural dio paso a una constelación de nuevas franquicias mediáticas que prolongan su legado discursivo en otros escenarios de conflicto.

Uno de los actores más visibles en esta nueva fase es el Estado Islámico de Khorasan (ISIS-K). Desde su base de operaciones en Afganistán, esta filial no solo ha reivindicado atentados espectaculares, como el ataque al aeropuerto de Kabul en 2021 o el atentado en la sala Crocus City Hall de Moscú en 2024, sino que ha desarrollado una narrativa propia, centrada en la traición de los talibanes, la

decadencia del islam suní tradicional, y la necesidad de una purga ideológica global. Su medio principal, Voice of Khurasan, combina textos doctrinales, vídeos operativos y panfletos en inglés y urdu, manteniendo una estética inspirada en Dabiq y Rumiya. El carácter juvenil y apocalíptico de su discurso demuestra que la estrategia de segmentación y dramatización simbólica permanece vigente (MEMRI, 2024).

En paralelo, otras filiales regionales han asumido un papel cada vez más relevante. En África occidental, la *Wilayat Gharb Ifriqiyyah*, rama del Estado Islámico de África Occidental tras escindirse en 2015 de Boko Haram, ha consolidado su propia estructura mediática mediante canales en Hausa e infografías multilingües difundidas por Telegram. La sofisticación de sus vídeos operativos, en los que se mezclan cánticos tradicionales con secuencias bélicas en primera persona como si se tratase de un videojuego, evidencia una profesionalización técnica heredada del Califato sirio, pero adaptada a entornos locales.

Una plataforma particularmente activa ha sido Al-Malahem Media, el brazo propagandístico de Al Qaeda en la Península Arábiga (AQAP). Aunque rivales doctrinales del Estado Islámico, comparten con ellos el uso sistemático de revistas (como Inspire) y vídeos tutoriales para fomentar ataques de lobos solitarios. En 2023, relanzaron el formato audiovisual de Inspire en un vídeo donde instaban a atacar contra “líderes de Silicon Valley” (MEMRI, 2023). El contenido, difundido a través de plataformas alternativas como Rocket.Chat o Threema, incluía instrucciones sobre explosivos caseros y recomendaciones de objetivos, replicando el modelo clásico de Daesh.

Del mismo modo, Al-Balagh Magazine, surgida en 2022, representa una nueva generación de portales ideológicos centrados en el adoctrinamiento juvenil. Su estilo recuerda a Rumiya, pero con un tono más pedagógico. Promueve un discurso de “reeducación islámica” que mezcla retórica salafista con alegorías del colapso moral de Occidente. Ha sido distribuida en Indonesia, Filipinas y Bangladesh, confirmando la internacionalización del discurso post-califato (Jihadology, 2022).

Cabe mencionar también el papel de The Global Islamic Media Front (GIMF), que ha actuado como repositorio de múltiples franquicias. Su función ya no es solo

difundir contenido, sino gestionar sinergias mediáticas entre grupos dispares, como Al Qaeda en el Magreb Islámico, el Ejército de Mahoma en Cachemira o el Turkistan Islamic Party (TIP), presente en la región uigur de China. Este último ha desarrollado una estética visual que recuerda a los primeros vídeos de Al Hayat, mezclando elementos culturales turcomanos con mensajes unificadores de yihad global.

El auge de estas plataformas ha sido posible gracias al uso sistemático de redes sociales descentralizadas y cifradas. Telegram sigue siendo el bastión principal del conglomerado yihadista, pero han surgido canales en Element, Riot, y servidores de Discord adaptados para esquivar la censura. Esta capacidad de supervivencia digital refuerza lo que Torres (2020) denomina “la hidra comunicativa del yihadismo post-califato” con múltiples cabezas discursivas que, aunque ideológicamente coordinadas, operan desde nichos territoriales y narrativos específicos.

Frente a esta fragmentación, resulta llamativo cómo se mantiene un mismo núcleo semántico: la legitimación de la violencia, la victimización colectiva, la utopía del Califato y la denuncia de la apostasía institucional. Cada grupo, cada wilaya, cada canal parece reinventar el relato sin romperlo. De hecho, muchas de las nuevas publicaciones como Sawt al-Hind, Nida e-Haq o Al-Fajr Media, reproducen incluso el diseño gráfico y los modelos narrativos de Dabiq, como si se tratara de una “franquicia comunicativa” que garantiza identidad, continuidad y eficacia.

En palabras de Sawt al-Hind (2021), se evidencia como para el Daesh de hoy en día, la difusión mediática de su ideario no constituye una estrategia secundaria, sino un pilar fundamental en la construcción de su legitimidad doctrinal y operativa:

¡Oh guerreros mediáticos del Califato! Uníos a vuestros hermanos y
permaneced a su lado en este terreno. Haced que la prueba quede clara ante
la gente.

¡Oh mensajero! Transmite lo que se te ha revelado de tu Señor. Si no
lo haces, no habrás transmitido Su mensaje.” (Corán, Surah Al-Ma’ida, 5:67)

Desde ese día, la Ummah de Muhammad (la paz sea con él) ha estado transmitiendo el mensaje del Profeta.

Hoy en día, el mayor medio de difusión es el de los medios de comunicación. Mientras que los incrédulos y apóstatas los usan para promover su falsedad, los seguidores del tawhid (monoteísmo puro) han alzado la bandera de la religión verdadera y se esfuerzan día y noche para erradicar el mal y las conspiraciones de los incrédulos y apóstatas.

Así pues, ¡oh partidarios del Califato en los medios! Uníos a vuestros hermanos y permaneced junto a ellos en este terreno. No escatiméis esfuerzos en difundir el monoteísmo puro y en rechazar la incredulidad y el politeísmo, cada clic vuestro tiene recompensa ante Allah y en el Día del Juicio lo veréis en la balanza de vuestras buenas obras (Sawt al-Hind, 2021).

Este fenómeno demuestra que la guerra narrativa no terminó con el colapso territorial de Daesh, sino que se reconfiguró en formas más móviles, multilingües y resilientes. Si antes el relato yihadista emanaba de un centro irradiador (Raqqah), hoy circula en red, a través de nodos que reproducen una misma cosmovisión, pero con matices locales. En este nuevo escenario, el desafío para los Estados y los servicios de inteligencia no es solo interrumpir canales o censurar contenidos, sino comprender cómo el relato muta, se adapta y seduce a nuevas generaciones.

8.3.7. La adopción del modelo comunicativo yihadista por otras organizaciones insurgentes

La eficacia de la estrategia comunicativa desplegada por el Estado Islámico durante su etapa califal no pasó desapercibida para otras organizaciones yihadistas globales. Grupos insurgentes, previamente centrados en operaciones militares convencionales o en formas rudimentarias de propaganda, han absorbido con rapidez y eficacia los códigos visuales, narrativos y tecnológicos desarrollados por Daesh, adaptándolos a sus respectivos contextos regionales y doctrinales.

Un caso paradigmático es el de Al Shabaab, la filial de Al Qaeda en Somalia, que ha transformado su aparato mediático en los últimos años. Su productora, Al-Kataib Foundation, ha abandonado el uso exclusivo del árabe para incorporar el inglés y el suajili, ampliando así su radio de acción y reclutamiento. Ha lanzado vídeos con fuerte carga simbólica, como el titulado "Usaama: Youth of the Nation", donde se muestra la ceremonia de graduación de una nueva brigada de muyahidines suicidas, con una puesta en escena que recuerda los documentales militares de Daesh (MEMRI, 2023). En ellos, se utilizan planos cenitales, efectos de sonido dramáticos, himnos épicos y testimonios de combatientes que refuerzan una narrativa de heroicidad y destino sagrado.

En el caso de Al Qaeda en la Península Arábiga (AQAP), su brazo propagandístico Al-Malahem Media ha mantenido un tono menos estridente que el de Daesh, pero no por ello menos sofisticado. A través de su revista Inspire, AQAP ha logrado renovar su formato digital con materiales interactivos, vídeos cortos y campañas en redes sociales cifradas. En 2024, por ejemplo, difundieron un vídeo titulado "Open Source Jihad: Lone Wolves Targeting the Elites", con instrucciones explícitas para atacar a figuras de renombre de las grandes corporaciones y mensajes que apelaban a un resentimiento social globalizado (MEMRI TV, 2024). Aquí, la conexión con el estilo Daesh es evidente: narrativas simples, imágenes impactantes y un enemigo claro.

La estrategia también ha sido replicada por el movimiento Talibán, que, tras el retorno al poder en Afganistán en 2021, ha desplegado una maquinaria mediática orientada a legitimarse internacionalmente. A través del Islamic Emirate Media Office, han difundido entrevistas con líderes, vídeos de reconstrucción, y panfletos doctrinales destinados a demostrar su supuesto respeto por la ley islámica y su

capacidad de gobernanza. Sin embargo, en paralelo, se ha mantenido una rama más radical que ha usado narrativas visuales de corte yihadista, especialmente cuando han querido distanciarse de acuerdos diplomáticos con Estados Unidos.

Mención especial merece el surgimiento de Al-Qaidah in the Indian Subcontinent (AQIS), cuyo boletín Nawa-e-Ghazwa-e-Hind se dirige directamente a las poblaciones musulmanas del sur de Asia. Su estructura semeja la de Rumiyaah o Dabiq, combinando retórica espiritual con llamadas a la acción violenta. AQIS ha empleado una estética sobria pero eficaz, con portadas que reproducen símbolos de la historia islámica regional y una distribución adaptada a plataformas censuradas en India o Pakistán.

En el norte de África, especialmente en el Sahel, Katiba Macina, ha empezado a utilizar herramientas de comunicación similares, aunque en un formato más rústico. Sus vídeos, publicados en canales yihadistas, adoptan el formato de testamento del mártir, mensajes a la comunidad y amenazas a los gobiernos locales, todo ello con un claro eco del modelo Daesh. El uso del francés como lengua secundaria revela la intención de llegar también a simpatizantes en Mali, Níger o Burkina Faso.

Lo notable de todos estos casos es que la profesionalización de la narrativa yihadista no está limitada a una organización concreta, sino que ha sido adoptada como un estándar por múltiples actores violentos. En un mundo interconectado, la marca propagandística del Daesh ha contaminado —en términos semióticos— el universo del islamismo radical armado. Incluso grupos como Hamas, con una base política más estructurada, han adoptado algunos recursos visuales y narrativos en sus campañas mediáticas: clips con música heroica, difusión de imágenes simbólicas de mártires, o creación de canales de mensajería directa para comunicarse con sus seguidores.

Otro ejemplo elocuente es el del Turkistan Islamic Party (TIP), activo en Xinjiang y zonas fronterizas con Pakistán. A través de vídeos difundidos en plataformas como Jihadology.net y Telegram, han emulado las fórmulas visuales del Estado Islámico: himnos marciales, dramatización de entrenamientos, invocaciones religiosas y el uso sistemático de subtítulos en árabe, chino e inglés. Su objetivo es doble: presentar al gobierno chino como enemigo de la umma y

atraer la simpatía de la diáspora uigur a su causa. Su estética, aunque menos refinada que la de Daesh, reproduce las claves del “storytelling yihadista”: la épica, el martirio y la lucha por la identidad.

En todos estos casos, el denominador común es la conciencia estratégica del poder del relato, de la imagen, del ritmo audiovisual y de la empatía ideológica. Como advierte Torres (2022), “la batalla contra el yihadismo ya no se libra únicamente en el campo físico, sino en el terreno de las percepciones, donde una historia bien contada puede valer más que cien fusiles”.

IX – LA RADICALIZACIÓN YIHADISTA: TEORÍAS, PROCESOS Y PERFILES DE LOS INDIVIDUOS

IX -LA RADICALIZACIÓN YIHADISTA: TEORÍAS, PROCESOS Y PERFILES DE LOS INDIVIDUOS

9.1. EL FENÓMENO DE LA RADICALIZACIÓN YIHADISTA EN EUROPA Y ESPAÑA

En los últimos años, la radicalización yihadista ha dejado de ser un fenómeno ajeno o distante para convertirse en una realidad que atraviesa las fronteras europeas con una alarmante persistencia. Si bien los atentados del 11 de septiembre de 2001 en Nueva York marcaron un antes y un después en la percepción global del terrorismo internacional, fueron las masacres de Madrid (2004), Londres (2005), París (2015) y Bruselas (2016) las que encendieron las alarmas sobre el arraigo y proliferación de células yihadistas en suelo europeo. Desde entonces, la Unión Europea ha intensificado sus esfuerzos en materia de inteligencia, prevención y cooperación antiterrorista, sin lograr, sin embargo, frenar completamente el fenómeno de la radicalización violenta, que ha sabido adaptarse a los nuevos tiempos mediante el uso estratégico de entornos digitales y la instrumentalización emocional de los jóvenes en situación de vulnerabilidad psicosocial.

En este escenario, España se ha consolidado como un actor clave tanto en la lucha contra el terrorismo de corte yihadista como en el análisis del fenómeno radicalizador. Tras los atentados de Barcelona y Cambrils en agosto de 2017 —los más graves en España desde el 11M— y la caída definitiva de Baghuz en 2019, último bastión del Califato de Daesh en Siria, se consolidó un nuevo paradigma en la lucha contra el yihadismo: el paso del terrorismo territorializado al terrorismo descentralizado, digital y doméstico. España, por su parte, no solo mantuvo su compromiso operativo, sino que reforzó su estrategia de vigilancia, anticipación y detención. Entre los años 2017 y 2025, según datos oficiales del Ministerio del Interior, se han desarrollado en territorio nacional 269 operaciones antiterroristas relacionadas con el yihadismo, que se han saldado con 447 detenidos (Ministerio del Interior, 2025).

A partir del año 2015, momento en que se introduce legalmente la figura del Agente Encubierto Informático mediante reforma de la Ley de Enjuiciamiento Criminal, se observa un incremento sostenido en el número de detenciones,

indicador del refuerzo de las capacidades investigativas y preventivas del Estado. No obstante, en 2018 se produce un descenso significativo, con apenas 29 arrestos. Este hecho coincide con el cerco militar que Daesh sufría en Siria e Iraq, especialmente tras la batalla de Deir ez-Zor a finales de 2017 y la posterior caída definitiva de Baghuz en 2019. Esta derrota marcó el fin del Califato territorial y dio origen a una nueva fase del terrorismo yihadista: la diáspora.

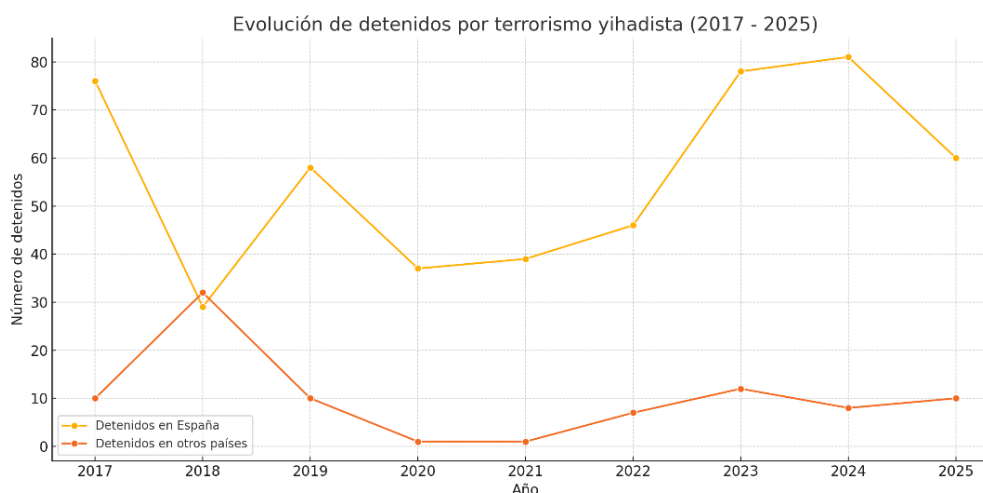
En los años siguientes, se produjo un aparente periodo de latencia en términos operativos, durante el cual se reconfiguraron redes, células y estructuras en el entorno europeo, alimentadas en parte por el regreso de los denominados “foreign fighters”, combatientes extranjeros que se habían trasladado a luchar a los territorios controlados por el Califato islámico de Daesh en Siria e Iraq, principalmente. A partir de 2023, sin embargo, se batían récords en el número de detenciones con la cifra más alta registrada hasta el momento, 78 detenciones; alcanzando un máximo histórico en 2024 con 81 detenidos. El año 2025, sin haber concluido aún, ya contabiliza 60 arrestos hasta mayo, lo cual anticipa una nueva oleada de radicalización activa y operativa. Todo ello confirma que el fenómeno yihadista ha entrado en una nueva fase expansiva, más difícil de detectar y combatir, tal y como muestran los siguientes gráficos y tablas estadísticas.

Figura 1: Evolución de detenidos por terrorismo yihadista tras la reforma de la LECrim del 2015 con el AEI como figura investigativa (2015 - 2025).



Elaboración propia (Ministerio del Interior, 2025).

Figura 2: Evolución de los detenidos por terrorismo yihadista desde los atentados terroristas de Cambrils y su comparativa con las detenciones de otros países. (2017 - 2025).



Elaboración propia (Ministerio del Interior, 2025).

Respecto a la edad, el 71 % de los detenidos tenía menos de 30 años en el momento de iniciar su radicalización, y un preocupante 23,4 % eran menores de edad. Esta tendencia al rejuvenecimiento ha sido documentada también por Vicente (2024), quien alerta del impacto que el entorno digital y la narrativa victimista están teniendo en adolescentes con identidades fragmentadas y escasa resiliencia emocional.

En cuanto al origen geográfico, los focos de radicalización se han concentrado en zonas específicas: Cataluña (36,6 %), Madrid (15,7 %), Ceuta (14,2 %) y Melilla (11,2 %), lo que sugiere la existencia de ecosistemas locales propicios a la radicalización, en los que confluyen dinámicas comunitarias, vínculos sociales previos y redes de adoctrinamiento persistentes (Vicente, 2024).

Las elevadas cifras evidenciadas, demuestran como la detección temprana de los procesos de radicalización violenta debe ser algo prioritario para garantizar la seguridad y paz pública de nuestras sociedades, debiendo atender sobremanera a los procesos de captación y radicalización que han envuelto a dichos individuos. Según el Observatorio Internacional de Estudios sobre Terrorismo (OIET, 2024), las operaciones policiales realizadas entre los años 2020 y 2024 destacan una evolución preocupante que “evidencia el creciente protagonismo de menores de edad,

ciudadanos nacionalizados, y conversos, muchos de ellos radicalizados desde su propio entorno doméstico a través de los entornos virtuales, redes sociales, videojuegos, canales de mensajería o foros clandestinos” (Igualada, 2024).

Un ejemplo paradigmático de esta transformación lo constituye la detención de cuatro adolescentes en Elche (Alicante) en diciembre de 2024, con edades comprendidas entre los 14 y los 17 años, acusados de planear atentados durante las fiestas navideñas contra lugares de culto cristiano como la basílica de Santa María (El Mundo, 2024). La operación reveló no solo el avanzado estado de radicalización de los implicados, sino también su vinculación con otras células digitales, el uso de canales cifrados y la existencia de manuales para la fabricación de explosivos (OIET, 2024). Hechos como estos nos obligan a replantear las estrategias preventivas desde una perspectiva integral que considere la dimensión sociológica, psicológica y tecnológica del proceso radicalizador.

Del mismo modo, en diciembre de 2023, tres menores —dos en Madrid y uno en Barcelona— fueron arrestados por adoctrinamiento y autocapacitación, habiendo interiorizado los postulados de Daesh a través de plataformas de videojuegos, en las que no solo justificaban la violencia terrorista, sino que compartían manuales para la confección de explosivos como el Triacetona Triperóxido, comúnmente conocido como TATP (OIET, 2023, p. 2). Este tipo de casos pone de relieve una mutación del proceso de captación, cada vez más descentralizado, autónomo, y difícil de detectar mediante los mecanismos tradicionales de inteligencia.

Aunque los atentados de Barcelona y Cambrils en agosto de 2017 marcaron el último gran acto de violencia yihadista ejecutado en territorio español, lo cierto es que la amenaza nunca ha cesado. Lejos de tratarse de estructuras jerárquicas como las que caracterizaban a Al Qaeda en sus orígenes, las nuevas formas de yihad operan mediante redes horizontales, microcélulas o incluso actores solitarios con altas dosis de autoadoctrinamiento, lo que en la literatura especializada se conoce como “yihadismo low-cost” (Reinares y García-Calvo, 2022, p. 14).

El perfil de los radicalizados, además, presenta elementos cada vez más diversos: incremento de las mujeres, menores de edad, conversos, individuos con problemas de salud mental, personas con antecedentes penales o con trayectorias vitales marcadas por la exclusión social, etc. No es extraño que, en muchas ocasiones, estas trayectorias desemboquen en un proceso de radicalización no solo

política o religiosa, sino también emocional, simbólica y existencial. Tal como advierte Fernando Reinares, “la radicalización yihadista opera como una narrativa de sentido, una promesa de pertenencia y misión para quienes carecen de anclajes en su entorno social inmediato” (Reinares, 2020, p. 77).

Las estadísticas recientes confirman esta tendencia: más del 60 % de los detenidos entre 2020 y 2025 en España consumían de forma habitual propaganda yihadista en línea, el 40 % de ellos la compartía activamente, y más del 25 % había considerado ejecutar un atentado (OIET, 2024). Asimismo, el porcentaje de menores implicados en actividades yihadistas ha aumentado un 220 % en los últimos cinco años, fenómeno que ha llevado a las autoridades a reforzar los sistemas de detección temprana y vigilancia digital en centros escolares, plataformas de videojuegos online y redes sociales de uso juvenil como podrían ser Tik Tok y Discord, entre otras (OIET, 2024).

La radicalización yihadista, por tanto, no puede comprenderse únicamente desde coordenadas de seguridad. Requiere una aproximación multidisciplinar, capaz de integrar las teorías del aprendizaje social, la psicología de la identidad, los marcos ideológicos salafistas, la narrativa del agravio y las vulnerabilidades estructurales que afectan a comunidades migrantes, musulmanas o convertidas. Por ello, en las siguientes secciones de este capítulo se abordarán en profundidad los modelos explicativos que han tratado de sistematizar este fenómeno, desde los pioneros como Silber y Bhatt hasta los enfoques más recientes centrados en la psicología moral, la teoría de los valores sagrados o las dinámicas de grupo.

9.2. MODELOS EXPLICATIVOS DE LA RADICALIZACIÓN YIHADISTA

La complejidad del proceso de radicalización yihadista ha exigido el desarrollo de modelos teóricos que permitan comprender sus diversas trayectorias, condicionantes individuales, sociales y simbólicos. Desde la psicología social, la criminología y los estudios sobre terrorismo se han consolidado diversas aproximaciones, entre las que destacan los modelos de Moghaddam (2005), Silber y Bhatt (2007), Sageman (2004), y las teorías de Sprinzak, Kruglanski, McCauley y Moskaleiko, entre otros. A continuación, se expone una síntesis crítica de los principales enfoques:

a) La escalera de la radicalización de Moghaddam.

Moghaddam (2005) propone una metáfora arquitectónica para explicar el camino hacia el terrorismo: una escalera de seis peldaños que parte de una base compartida por toda la sociedad. En el primer nivel se sitúa la percepción subjetiva de injusticia, agravios y exclusión. A medida que el individuo asciende, se aleja de estrategias de acción convencionales y abraza visiones dicotómicas del mundo, hasta alcanzar el punto en el que la violencia se convierte en un mandato moral. Este modelo destaca que no todas las personas que se sienten agraviadas escalan, pero sí subraya que quienes lo hacen comparten patrones cognitivos similares: alienación, deslegitimación del orden social y búsqueda de significado (Galvis, 2021, pp. 85-87).

Un ejemplo ilustrativo es el caso de Abdelbaki Es Satty, el imán de Ripoll y cerebro ideológico de los atentados de Barcelona y Cambrils en 2017. Su trayectoria vital refleja los peldaños descritos por Moghaddam (2006), pues pasó de experimentar una situación de exclusión social y resentimiento por su condena penal y sus dificultades para integrarse en la comunidad islámica, a abrazar una narrativa dicotómica y salafista radical. En un contexto de clandestinidad, adoctrinó a un grupo de jóvenes marroquíes de segunda generación, transmitiéndoles la idea de que la violencia yihadista era un deber moral. Su discurso de ruptura con la sociedad occidental y su reinterpretación del islam como mandato combativo encarnan perfectamente los niveles superiores de la escalera, en los que se justifica la violencia como medio legítimo para reivindicar un orden nuevo (Reinares y García-Calvo, 2022, pp. 24-28).

b) El modelo de radicalización en cuatro fases de Silber y Bhatt.

Silber y Bhatt (2007), en un informe del NYPD, identifican cuatro fases: pre-radicalización, autoidentificación, adoctrinamiento y yihadización. El modelo fue construido a partir de casos judicializados en EE. UU. y señala que el acceso a mensajes ideológicos yihadistas online, el contacto con figuras carismáticas, y la progresiva desvinculación del entorno previo son constantes en estos procesos. Aunque ha sido criticado por su reduccionismo, sigue siendo un referente operativo en cuerpos de seguridad.

Un ejemplo práctico en el contexto español que puede ilustrar este modelo es el caso de las hermanas detenidas en Alcorcón en mayo de 2025. Ambas, de 19 y 21 años, fueron arrestadas por la Policía Nacional por delitos de adoctrinamiento terrorista. Durante la etapa de pre-radicalización, llevaban una vida aparentemente normal dentro de una familia musulmana moderada. En la fase de autoidentificación, comenzaron a interesarse por el salafismo a través de plataformas en línea. Posteriormente, en la etapa de adoctrinamiento, crearon una plataforma digital donde difundían los postulados de Daesh dirigidos a mujeres jóvenes, valiéndose de un discurso supuestamente religioso. Finalmente, en la fase de yihadización, asumieron el rol de adoctrinadoras activas, buscando convencer a otras mujeres de unirse a la causa yihadista, todo ello desde una estrategia de clandestinidad y uso intensivo de tecnologías de cifrado y anonimato (OIET, 2024).

c) La red social como espacio de radicalización (Sageman).

Sageman (2004) sostiene que la radicalización no ocurre principalmente por adoctrinamiento doctrinal, sino por el deseo de pertenencia a un grupo. Desde su perspectiva, los procesos de socialización y la dinámica grupal son el motor real de la radicalización violenta. Es en las redes informales donde los individuos encuentran un sentido de identidad, respeto y misión. El caso del grupo que perpetró los atentados de Madrid en 2004 valida esta hipótesis: ninguno de sus miembros tenía una formación islámica profunda, pero sí un fuerte vínculo grupal basado en la amistad, el resentimiento compartido y una narrativa de venganza (Reinares, 2014).

d) Teoría de la deslegitimación (Sprinzak).

Sprinzak (1991) distingue entre deslegitimación transformacional, extensiva y dividida. En la primera, el individuo se separa psicológicamente del orden legal y moral existente; en la segunda, esta ruptura se amplifica y abarca instituciones enteras; y en la tercera, el odio se dirige a grupos concretos percibidos como amenaza. Esta teoría resulta útil para explicar por qué algunos individuos formados en contextos democráticos terminan defendiendo modelos totalitarios, como el Califato.

Un ejemplo claro lo encontramos en el caso de Mohamed Houli Chemlal, superviviente del atentado de Alcanar vinculado a los ataques de Barcelona y Cambrils en 2017. Houli pasó de una fase inicial de alienación individual a una progresiva deslegitimación del Estado español y sus instituciones. Primero rompió con las normas sociales de su entorno (fase transformacional), luego adoptó un discurso de rechazo global hacia las estructuras políticas y religiosas occidentales (fase extensiva), y finalmente canalizó su odio contra colectivos específicos a través de la planificación de acciones terroristas dirigidas a civiles inocentes, considerados por el grupo como enemigos del islam (fase dividida). Este proceso refleja la genealogía estructural progresiva descrita por Sprinzak en su teoría de la deslegitimación (Reinares y García-Calvo, 2022, pp. 31-34).

e) El modelo 3N: Necesidad, Narrativa y Red.

Kruglanski y Webber (2017) sintetizan diversos factores psicológicos bajo tres grandes dimensiones: la necesidad de significado, la narrativa que justifica la violencia y la red que sostiene e impulsa dicha narrativa. Este modelo ha ganado reconocimiento por su capacidad para explicar tanto la radicalización individual como la grupal. Destaca que la radicalización puede ser reactiva (ante agravios personales o colectivos) o proactiva (búsqueda de estatus, heroísmo, trascendencia). Cuando el entorno ofrece una narrativa coherente y un grupo de referencia que premia la violencia como virtud moral, la radicalización se intensifica (Kruglanski et al., 2014).

Un caso paradigmático es el de un joven marroquí de 22 años detenido en Ceuta en abril de 2023, quien tras experimentar una profunda crisis personal asociada al desempleo y al rechazo social, comenzó a consumir masivamente propaganda de Daesh a través de Telegram y foros salafistas. La narrativa ofrecida por el grupo le proporcionó una identidad heroica y trascendente, mientras que su red digital de apoyo reforzó la validación de su radicalización. Llegó incluso a realizar un juramento de fidelidad (*bayah*) al líder del Estado Islámico y estaba recopilando materiales para fabricar artefactos explosivos (OIET, 2023, pp. 5-6).

f) Modelos complementarios: teorías psicosociales y valores sagrados.

Teorías como la de la fusión de identidad (Swann et al., 2015), la teoría de la reducción de la incertidumbre (Hogg, 2007) o el modelo de la violencia moral (Fiske & Rai, 2014) complementan el análisis de los anteriores.

La teoría de la fusión de identidad plantea que los individuos pueden llegar a fusionar completamente su identidad personal con la grupal, de modo que los intereses del grupo se sienten como propios, lo que justifica el sacrificio extremo.

La teoría de la reducción de la incertidumbre, por su parte, sostiene que, en contextos de ambigüedad o exclusión, las personas tienden a adherirse a grupos con normas claras y rígidas, como los grupos yihadistas.

Finalmente, el modelo de la violencia moral explica cómo ciertas culturas grupales pueden justificar la violencia como expresión de valores profundamente compartidos y defendidos. Todas convergen en señalar que los individuos que adoptan la violencia como herramienta última no están necesariamente trastornados, sino que actúan con base en una racionalidad instrumental, moral o grupal (Giner, 2020).

En conjunto, estos modelos permiten una aproximación holística al fenómeno de la radicalización yihadista. Ninguno es suficiente por sí solo, pero combinados ofrecen un marco de comprensión que resulta imprescindible para cualquier estrategia de prevención y desradicalización.

9.3. FACTORES PSICOSOCIALES, IDENTITARIOS Y CONTEXTUALES EN LA RADICALIZACIÓN YIHADISTA

Comprender la radicalización yihadista exige analizar no solo modelos teóricos abstractos, sino también los factores concretos que, a nivel individual y grupal, predisponen a ciertos sujetos a adoptar ideologías violentas. Estos factores psicosociales no actúan de forma aislada, sino que se entrelazan en contextos estructurales de exclusión, identidad fracturada y dinámicas de grupo intensivas, generando un terreno fértil para el adoctrinamiento y la acción violenta.

Uno de los factores más determinantes es la crisis identitaria, especialmente entre jóvenes musulmanes de segunda generación en Europa. A menudo atrapados entre dos mundos, por un lado, la cultura de origen familiar y por otro la sociedad del país de acogida, muchos no logran integrarse plenamente en ninguno. Este desarraigo se traduce en una sensación de invisibilidad o alienación, que es hábilmente explotada por los discursos yihadistas para ofrecer una identidad fuerte, pura y combativa (Moyano, 2013). La narrativa salafista-yihadista proporciona así una respuesta a su vacío existencial, convirtiéndolos en mártires potenciales de una causa que otorga sentido y pertenencia.

La exclusión social y económica también actúa como catalizador. Si bien no todos los radicalizados proceden de entornos marginales, una parte significativa ha vivido experiencias de discriminación, desempleo, fracaso escolar o violencia institucional. Estas vivencias alimentan una narrativa del agravio y la injusticia que refuerza el sentimiento de victimización colectiva. En palabras de Reinares (2014), "la radicalización es un proceso en el que el individuo interpreta su biografía como parte de una tragedia colectiva, y ve en la yihad una forma de venganza simbólica" (p. 89).

Otro componente esencial es la influencia del grupo de pares. Como demostró Sageman (2004), muchos yihadistas no se radicalizan en soledad, sino en pequeños núcleos donde se refuerzan mutuamente sus creencias. La lealtad al grupo, la admiración por miembros más comprometidos y la presión por no quedar rezagado moralmente generan una dinámica de escalada que culmina en la acción violenta. Esta dimensión meso grupal, frecuentemente ignorada, resulta clave para entender por qué la radicalización se produce con tanta rapidez en contextos cerrados y homogéneos.

En este sentido, el caso de los detenidos en 2022 en Melilla, un grupo de cinco jóvenes sin antecedentes penales pero con fuerte vinculación amistosa y vecinal, es paradigmático. Según informes policiales, el grupo pasó en apenas seis meses de compartir vídeos de Dabiq y Rumiyah a planificar ataques con explosivos improvisados (OIET, 2022, pp. 4-5). Ninguno actuaba como líder ideológico, pero la cohesión del grupo y la dinámica de refuerzo mutuo aceleraron el proceso de radicalización colectiva.

Finalmente, cabe destacar el papel del entorno político y mediático. Discursos islamófobos, políticas migratorias restrictivas y la estigmatización generalizada de

las comunidades musulmanas contribuyen a la polarización social y alimentan la narrativa de guerra contra el islam. Tal entorno facilita el discurso binario nosotros/ellos que está en la base de toda ideología extremista.

Por todo ello, comprender estos factores no es un ejercicio teórico, sino que son la base investigativa en la que deben apoyarse las FCSE y sobre la que las Administraciones deben diseñar políticas de prevención eficaces, sensibles a la dimensión humana de la radicalización y al contexto en el que esta se gesta.

9.4. EL PAPEL DEL ESPACIO DIGITAL EN LA RADICALIZACIÓN, CAPTACIÓN Y ADOCTRINAMIENTO DEL INDIVIDUO

La irrupción de Internet y el desarrollo de tecnologías digitales han transformado profundamente las dinámicas de captación y radicalización yihadista. Para comprender esta evolución, resulta útil la teoría del "militante autodidacta" formulada por Sageman (2008), que describe cómo individuos aislados pueden radicalizarse mediante contenidos digitales sin contacto físico con estructuras jerárquicas. Según Sageman, la radicalización online es un proceso en red, descentralizado, en el que la interacción con ideologías extremas a través de medios digitales suple el papel del mentor presencial, permitiendo al sujeto construir una identidad militante autónoma pero alineada con los postulados del yihadismo global. Esta teoría resulta especialmente pertinente para explicar fenómenos contemporáneos como los lobos solitarios hiperconectados o las células digitales sin liderazgo vertical claro. El entorno virtual no es solo un canal de comunicación, sino un auténtico espacio de socialización ideológica, formación doctrinal, reclutamiento operativo y adoctrinamiento emocional. Desde los primeros foros de Al Qaeda en la red hasta la sofisticada maquinaria propagandística de Daesh, el ciberespacio ha operado como un campo de batalla narrativo y simbólico.

Las plataformas empleadas han ido evolucionando conforme se intensificaba la presión policial y los mecanismos de detección. De los foros abiertos como Ansar al-Mujahideen se pasó a redes sociales generalistas como Facebook, Twitter o YouTube; y posteriormente, ante los bloqueos y cierres de cuentas, a aplicaciones cifradas como Whatsapp, Telegram, Rocket.Chat o TamTam. En la actualidad, el

uso de canales de videojuegos online, servidores de Discord, transmisiones streaming en directo en plataformas marginales y nuevamente Telegram, han abierto nuevas rutas de captación más difíciles de monitorizar (Driessen et al., 2025).

El valor del entorno virtual reside no solo en su capacidad de difusión, sino en su eficacia para construir comunidades simbólicas. Los usuarios no acceden únicamente a contenidos, sino que interactúan, comparten, producen y refuerzan mutuamente sus creencias. El concepto de "cámara de eco", formulado inicialmente por Sunstein (2001), es especialmente útil para describir este fenómeno: los mensajes se amplifican dentro de entornos ideológicamente homogéneos, bloqueando voces disidentes y consolidando una visión binaria del mundo.

Los procesos de autoadocctrinamiento online han adquirido una centralidad indiscutible. La disponibilidad inmediata de vídeos, manuales, sermones incendiarios, instrucciones operativas y testimonios de mártires configura una oferta ideológica total, accesible sin intermediarios. Tal como ha documentado el Observatorio Internacional de Estudios sobre Terrorismo (OIET, 2024), más del 70% de los detenidos por delitos relacionados con el yihadismo en España en los últimos tres años habían iniciado su proceso de radicalización en solitario a través de medios digitales.

Un caso emblemático es el de un joven detenido en Sabadell en enero de 2024. Aislado socialmente y con antecedentes de salud mental, había consumido decenas de vídeos de Al Hayat y Rumiya en canales de Telegram. No formaba parte de ninguna célula, pero había confeccionado un plan detallado para atacar contra una comisaría local. Su caso representa la figura del "actor solitario conectado digitalmente", cada vez más habitual en el panorama europeo (OIET, 2024, p. 3).

Junto al autoadocctrinamiento, los procesos de captación dirigidos siguen activos. Se han detectado cuentas falsas en TikTok, perfiles en Instagram con estética modernista, y canales de videojuegos online donde usuarios aparentemente anónimos inician conversaciones privadas para detectar vulnerabilidades emocionales, especialmente en adolescentes. La combinación de propaganda espectacular, gamificación, victimismo musulmán global y promesas de hermandad configuran un cóctel atractivo para perfiles jóvenes en busca de identidad y propósito.

Ante este escenario, la radicalización online y sobre todo ante la creciente oleada de menores radicalizados (Requeijo, 2024), se convierte en un reto no solo técnico, sino político y cultural. La detección de señales tempranas, la educación digital crítica, la cooperación con plataformas tecnológicas y la sensibilización de familias y centros educativos son pilares fundamentales de cualquier estrategia de prevención eficaz.

9.5. REVISIÓN CRÍTICA SOBRE LOS PROGRAMAS DE PREVENCIÓN Y DESRADICALIZACIÓN

La expansión del yihadismo en Europa ha impulsado el desarrollo de múltiples estrategias orientadas a la prevención y desradicalización. No obstante, su implementación y eficacia han sido dispares según el país, el enfoque institucional adoptado y la articulación con actores sociales. Esta sección examina los modelos aplicados en el ámbito europeo y español, evaluando sus fortalezas, limitaciones y retos actuales.

- **Modelos europeos:**

En Europa, países como Reino Unido, Alemania y Francia han diseñado estrategias integrales desde hace más de una década. El modelo británico "Prevent" —dentro de la estrategia CONTEST— ha sido pionero, centrado en identificar signos tempranos de radicalización y ofrecer alternativas educativas o laborales. Sin embargo, ha sido fuertemente criticado por sectores musulmanes que lo perciben como una herramienta de estigmatización (Qurashi, 2018).

Alemania ha apostado por modelos descentralizados gestionados por ONGs, con énfasis en la intervención comunitaria, la mediación intercultural y el seguimiento individualizado. El programa HAYAT, desarrollado por la ONG EXIT-Deutschland, ofrece apoyo a familias con miembros en proceso de radicalización. Francia, por su parte, ha privilegiado una respuesta securitaria, con internamiento de radicalizados, cierre de mezquitas y vigilancia sistemática, aunque con escasa evaluación pública de sus resultados (Khosrokhavar, 2017).

- **Estrategias españolas:**

España ha ido desarrollando progresivamente su marco preventivo y de intervención. El Plan Estratégico Nacional de Lucha contra la Radicalización Violenta (PEN-LCRV), aprobado en 2015 y actualizado en 2020, establece líneas de actuación en ámbitos como la detección temprana, la cooperación institucional, la educación y la participación comunitaria. Incluye también la figura del "punto focal local", un agente de enlace entre instituciones y comunidades (Ministerio del Interior, 2020).

A nivel autonómico y municipal, destacan programas como el de la Generalitat de Cataluña (PICV) y experiencias piloto en Ceuta y Melilla, orientadas al trabajo con jóvenes en riesgo. Instituciones penitenciarias también han desarrollado programas específicos para internos por delitos yihadistas, aunque con escasa transparencia sobre sus resultados reales (Ballester, 2021).

Sin embargo, a pesar de los esfuerzos, los datos disponibles indican una eficacia limitada de los programas de desradicalización. Diversos informes señalan que los procesos de abandono de la violencia son largos, complejos y muy sensibles al contexto. La mayoría de iniciativas se centran en el individuo radicalizado, descuidando los factores estructurales o comunitarios que facilitaron su captación. Además, muchos programas carecen de mecanismos rigurosos de evaluación, y su éxito se mide en términos excesivamente simplistas, como la ausencia de reincidencia en un periodo concreto (El-Said, 2015).

El propio Ministerio del Interior español reconocía en su evaluación interna de 2022 que se requiere mayor inversión en formación especializada, acompañamiento postpenitenciario y coordinación entre organismos. Por otro lado, los discursos públicos centrados en la amenaza, más que en la inclusión, dificultan el desarrollo de estrategias preventivas efectivas y sostenibles.

En suma, los programas existentes son necesarios pero insuficientes. Requieren una reformulación que combine la vigilancia con la integración, el seguimiento individualizado con el trabajo comunitario, y la securitización con políticas sociales.

Una de las dimensiones más preocupantes es el relativo fracaso de los programas de desradicalización en el ámbito penitenciario. La llamada

'radicalización intramuros' no solo no ha sido contenida, sino que ha experimentado un crecimiento sostenido. Casos como el de la Operación Dihan, instruida por la Audiencia Nacional en 2021 y culminada con la sentencia 955/2025, evidencian cómo internos ya condenados por delitos de terrorismo han ejercido de adoctrinadores en prisión, creando núcleos salafistas y captando a otros reclusos comunes. La red desmantelada en esa operación llegó a planear atentados y difundir propaganda yihadista desde el interior de centros penitenciarios como Topas o Mansilla de las Mulas (OIET, 2021).

A este fenómeno contribuye una combinación de factores: la falta de personal especializado, la dificultad de controlar los discursos religiosos, la sobrecarga de las unidades de seguimiento y el uso de la prisión como entorno de reafiliación identitaria. Como alertó un informe interno de Instituciones Penitenciarias, existen decenas de internos en situación de riesgo de radicalización sin un programa de intervención individualizada, lo que convierte a la prisión en un espacio de socialización yihadista más que en un ámbito de reinserción (El Mundo, 2021).

La evidencia empírica exige replantear el modelo actual: no basta con estrategias pasivas de observación o programas genéricos. Se requieren metodologías específicas, equipos mixtos formados por criminólogos, psicólogos e imanes acreditados, y un sistema de evaluación realista basado en indicadores cualitativos de desistencia y cambio ideológico. Solo así será posible abordar con realismo y eficacia el complejo fenómeno de la radicalización yihadista.

**X – LA FIGURA DEL
AGENTE ENCUBIERTO EN EL
ORDENAMIENTO JURÍDICO
ESPAÑOL**

X - LA FIGURA DEL AGENTE ENCUBIERTO EN EL ORDENAMIENTO JURÍDICO ESPAÑOL

10.1. EVOLUCIÓN LEGISLATIVA Y CONTEXTO NORMATIVO

10.1.1. El Convenio de Budapest y la cooperación internacional en ciberdelincuencia

La configuración de un orden jurídico capaz de afrontar los desafíos de la ciberdelincuencia ha exigido, desde sus orígenes, una concepción supranacional del delito y de la persecución penal. Las redes criminales no conocen fronteras; los actos delictivos se materializan en múltiples países al unísono, las direcciones IP se ocultan bajo capas de ocultación transnacionales; los atacantes operan desde servidores localizados en países sin tratados de extradición ni cooperación internacional, etc. En este contexto, la respuesta aislada de los Estados resulta claramente insuficiente, por lo que la cooperación internacional se ha erigido como un pilar esencial en la lucha contra el delito digital.

Este es el fundamento que inspira la adopción del Convenio sobre la Ciberdelincuencia del Consejo de Europa, firmado en Budapest el 23 de noviembre de 2001. Considerado el primer instrumento internacional vinculante en la materia, establece un marco común para la tipificación de delitos cometidos mediante sistemas informáticos y para la persecución eficaz de dichos delitos a través de la cooperación interestatal.

Según establece su artículo 1, el objetivo general del convenio es el de “perseguir una política penal común destinada a la protección de la sociedad frente a la ciberdelincuencia, en particular mediante la adopción de legislación adecuada y la mejora de la cooperación internacional” (Consejo de Europa, 2001). Esta formulación no es retórica, sino que se trata de una verdadera hoja de ruta para los Estados firmantes, quienes se comprometen no solo a armonizar sus tipos penales, sino a establecer mecanismos eficaces de investigación y asistencia recíproca.

En su artículo 2, el convenio obliga a los Estados a penalizar el acceso ilícito a sistemas informáticos, mientras que el artículo 5 establece la criminalización de la interferencia en datos, y el artículo 6 aborda el uso indebido de dispositivos. La

sección segunda del convenio se dedica íntegramente al desarrollo de “medidas procesales especiales”, entre ellas la obligación de “adoptar las medidas legislativas necesarias para establecer la conservación rápida de datos informatizados almacenados”, el acceso a datos almacenados, así como la “interceptación de datos de contenido y datos de tráfico en tiempo real” (Consejo de Europa, 2001, arts. 16–21).

No menos relevante es el contenido del Capítulo III, dedicado a la cooperación internacional. Allí se impone a los Estados signatarios la obligación de prestar la asistencia jurídica recíproca más amplia posible, incluso en ausencia de tratado bilateral, en materia de “conservación de datos, acceso transfronterizo, investigación conjunta y notificación inmediata de infracciones” (Consejo de Europa, 2001, art. 25).

La ambición del convenio no radica solo en su contenido técnico, sino en su vocación de universalidad jurídica. Aunque originado en el seno del Consejo de Europa, está abierto a la adhesión de países no europeos, y cuenta a día de hoy con más de 70 Estados parte. Entre ellos figuran Estados Unidos, Japón, Argentina, Chile, Colombia y Brasil, lo que demuestra su condición de estándar global en materia de cibercriminalidad.

España firmó el convenio el 23 de noviembre de 2001, aunque no lo ratificó hasta el año 2010, momento en el que entró en vigor con su publicación en el Boletín Oficial del Estado (BOE, 2010). Este retraso refleja una tendencia general en los ordenamientos jurídicos a adaptarse lentamente a realidades tecnológicas que avanzan a un ritmo más acelerado que las reformas normativas. No obstante, una vez ratificado, el convenio sirvió de base estructural para las sucesivas reformas del Código Penal y la Ley de Enjuiciamiento Criminal, especialmente las de los años 2010, 2015 y 2020.

En palabras de López-Muñoz (2020), “el Convenio de Budapest representa la primera tentativa seria y jurídicamente coherente de dotar al orden internacional de una gramática penal común en la lucha contra el crimen electrónico” (p. 92). Gracias a este tratado, instituciones como Europol, Eurojust y las Fiscalías especializadas han podido colaborar más estrechamente en la persecución de delitos tan diversos como el terrorismo, la pornografía infantil, los delitos de hacking, el ciberespionaje o el fraude económico digital a gran escala

Por tanto, explicar la evolución normativa sufrida hasta la génesis del AEI no puede entenderse sin esta base supranacional del Convenio de Budapest, que actúa como base operativa nacional sobre un compromiso internacional de colaboración y adecuación normativa asumida por el Estado firmante. Su legalidad, su utilidad y sus límites se proyectan en función de las obligaciones que se asumen tras su adhesión, cuya influencia alcanza no solo al legislador nacional, sino también al juez de instrucción y al fiscal que debe operar en el complejo mundo de la delincuencia a través del espacio digital.

10.1.2. Reformas clave del ordenamiento jurídico español: Ley Orgánica 5/2010, Ley Orgánica 2/2015 y Ley Orgánica 13/2015

El proceso de adaptación del ordenamiento jurídico español a los desafíos de la ciberdelincuencia no ha sido ni inmediato ni uniforme. Ha requerido un ejercicio legislativo pausado, a menudo reactivo, marcado por una constante tensión entre los principios garantistas del Estado de Derecho y las exigencias operativas de la lucha contra un crimen cada vez más deslocalizado, descentralizado y digital. Como primer paso en esa evolución, destaca la Ley Orgánica 5/2010, de 22 de junio, por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal, que introdujo reformas sustanciales en el Código Penal español. Esta norma constituyó el primer intento serio de trasposición de los principios contenidos en el Convenio de Budapest, aunque sin agotar aún la problemática emergente del terrorismo yihadista contemporáneo.

La exposición de motivos de la LO 5/2010 advertía con claridad que “la irrupción de las tecnologías de la información ha supuesto una transformación profunda en el modo de delinquir, facilitando nuevos escenarios para la criminalidad organizada y transnacional” (BOE, 2010). En consonancia con este diagnóstico, se procedió a reformular las figuras delictivas que involucran medios informáticos, tanto en el ámbito patrimonial como en el de la privacidad y la integridad de los sistemas.

Uno de los artículos reformados fue el artículo 248 CP, que en su nueva redacción ampliaba la noción de estafa para incluir los supuestos de fraude informático. Según su tenor literal: “También se consideran reos de estafa los que,

con ánimo de lucro y valiéndose de alguna manipulación informática o artificio semejante, consigan una transferencia no consentida de cualquier activo patrimonial en perjuicio de tercero” (BOE, 2010, art. 248.2).

Con ello, el legislador reconocía por primera vez que el engaño puede no provenir de una persona física, sino de una interfaz digital que tiene como objetivo la estafa de los usuarios mediante técnicas de phishing o ingeniería social a través de la manipulación o la simulación fraudulenta de páginas webs aparentemente lícitas, que en realidad lo que hacen es suplantar estas webs de forma tan excelsa que en gran medida pueden inducir al error humano. Este cambio conceptual supuso un giro doctrinal relevante en la interpretación del dolo y del perjuicio en el ámbito digital.

Igualmente significativa fue la nueva redacción del artículo 264 CP, que sanciona los daños informáticos: “El que, por cualquier medio, sin autorización y de manera grave, borre, dañe, deteriore, altere, suprima o haga inaccesibles datos informáticos, programas informáticos o documentos electrónicos ajenos, será castigado con la pena de prisión de seis meses a tres años” (BOE, 2010).

Por primera vez se introdujo la noción de daño no físico, es decir, la afectación directa de bienes intangibles como datos, archivos informáticos, programas o sistemas, independientemente de si existía destrucción material. Esta innovación permitió perseguir acciones como ataques DDoS, infecciones por malware como podrían ser los troyanos, virus o el tan de moda ransomware⁷, así como intrusiones deliberadas en servidores protegidos.

Finalmente, se reforzó la protección de la intimidad digital mediante la modificación del artículo 197 y siguientes, tipificando conductas como la obtención de información sin consentimiento mediante acceso remoto, o la difusión de contenidos privados vulnerando claves o contraseñas. El nuevo artículo 197 bis, incorporado en esta reforma, ampliaba el perímetro penal: “Será castigado con la

⁷ El ransomware es un software malicioso que una vez es detonado por el atacante en la infraestructura de la víctima, procede a encriptar todos sus archivos e información, impidiendo su acceso a los usuarios legítimos, a quienes solicitan el pago de una cuantía económica para la obtención de la clave de descifrado de sus archivos. Este tipo de extorsión cibernética ha ido evolucionando a lo largo de los últimos años a través de otra serie de actividades delictivas conexas, como son los ataques de denegación de servicio distribuido, las coacciones y la extorsión directa a las víctimas, la venta en el mercado negro de los datos y la información clasificada exfiltrada, etc.

pena de prisión de seis meses a dos años el que, por cualquier medio, vulnerando medidas de seguridad, acceda sin autorización a datos personales almacenados en ficheros o sistemas informatizados” (BOE, 2010).

Esta previsión resultó fundamental para perseguir conductas delictivas de hacking (cracking) no necesariamente vinculadas al ánimo de lucro, como las realizadas por hacktivistas, insiders o grupos de ciberespionaje, así como los diferentes actores de la amenaza que copan a día de hoy el underground del cibercrimen, ransomware as a service⁸, initial access broker, etc.

En definitiva, la LO 5/2010 constituyó una respuesta parcial, pero pionera. Aún no se abordaba de manera directa el fenómeno del terrorismo yihadista digital, ni la figura del agente encubierto informático, pero sí se sentaron las bases doctrinales y jurídicas para una comprensión penal del cibercrimen, inaugurando una nueva etapa legislativa.

Tras ello en 2015, en un contexto marcado por la expansión del yihadismo global, el auge del Estado Islámico y el reclutamiento y adoctrinamiento masivo de combatientes extranjeros a través de plataformas digitales. En palabras del entonces ministro del Interior, Jorge Fernández Díaz, la amenaza se caracterizaba por “su carácter difuso, transfronterizo y descentralizado, con un altísimo grado de instrumentalización del entorno digital para captar, adoctrinar, entrenar y dirigir atentados” (Congreso de los Diputados, 2015), se promulgó la Ley Orgánica 2/2015, de 30 de marzo, por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal, en materia de delitos de terrorismo. Esta constatación motivó una reforma profunda del Título XXII del Código Penal, que pasó a incorporar por primera vez tipos penales directamente vinculados al ciberterrorismo, el adoctrinamiento pasivo y el auto adiestramiento.

Así el artículo Artículo 573 del Código Penal considera delito de terrorismo:

⁸ El ransomware as a service es un modelo de negocio delictivo en el que los desarrolladores de ransomware se convierten en una organización matriz delictiva, y venden o alquilan su malware a otros grupos criminales que se denominan afiliados, a través de una suscripción o un tanto por ciento del monto económico que obtengan de sus extorsiones por el cifrado y exfiltración de datos que realizan a sus víctimas.

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

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

2) Alterar gravemente la paz pública.

3) Desestabilizar gravemente el funcionamiento de una organización internacional.

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

2. Se considerarán igualmente delitos de terrorismo los delitos informáticos tipificados en los artículos 197 bis y 197 ter y 264 a 264 quater

cuando los hechos se cometan con alguna de las finalidades a las que se refiere el apartado anterior.

3. Asimismo, tendrán la consideración de delitos de terrorismo el resto de los delitos tipificados en este Capítulo. (BOE, 2015)

En concordancia a lo anterior, el artículo 575 CP, en su nueva redacción, es especialmente ilustrativo de esta lógica preventiva por parte del legislador, pues ya en el preámbulo justifica que:

El artículo 575 tipifica el adoctrinamiento y el adiestramiento militar o de combate o en el manejo de toda clase de armas y explosivos, incluyendo expresamente el adoctrinamiento y adiestramiento pasivo, con especial mención al que se realiza a través de internet o de servicios de comunicación accesibles al público, que exige, para ser considerado delito, una nota de habitualidad y un elemento finalista que no es otro que estar dirigido a incorporarse a una organización terrorista, colaborar con ella o perseguir sus fines. También se tipifica en este precepto el fenómeno de los combatientes terroristas extranjeros, esto es, quienes para integrarse o colaborar con una organización terrorista o para cometer un delito de terrorismo se desplacen al extranjero. (BOE, 2015).

Y posteriormente precisando su redacción conforme a los siguientes preceptos:

1. Será castigado con la pena de prisión de dos a cinco años quien, con la finalidad de capacitarse para llevar a cabo cualquiera de los delitos tipificados en este Capítulo, reciba adoctrinamiento o adiestramiento militar o de combate, o en técnicas de desarrollo de armas químicas o biológicas, de elaboración o preparación de sustancias o aparatos explosivos, inflamables, incendiarios o asfixiantes, o específicamente destinados a facilitar la comisión de alguna de tales infracciones.” (BOE, 2015).

2. Con la misma pena [prisión de dos a cinco años] se castigará a quien, con la misma finalidad de capacitarse para cometer alguno de los delitos tipificados en este Capítulo, lleve a cabo por sí mismo cualquiera de las actividades previstas en el apartado anterior [reciba adoctrinamiento o adiestramiento militar o de combate, o en técnicas de desarrollo de armas químicas o biológicas, de elaboración o preparación de sustancias o aparatos explosivos, inflamables, incendiarios o asfixiantes, o específicamente destinados a facilitar la comisión de alguna de tales infracciones].

Se entenderá que comete este delito quien, con tal finalidad, acceda de manera habitual a uno o varios servicios de comunicación accesibles al

público en línea o contenidos accesibles a través de internet o de un servicio de comunicaciones electrónicas cuyos contenidos estén dirigidos o resulten idóneos para incitar a la incorporación a una organización o grupo terrorista, o a colaborar con cualquiera de ellos o en sus fines. Los hechos se entenderán cometidos en España cuando se acceda a los contenidos desde el territorio español.

Asimismo, se entenderá que comete este delito quien, con la misma finalidad, adquiera o tenga en su poder documentos que estén dirigidos o, por su contenido, resulten idóneos para incitar a la incorporación a una organización o grupo terrorista o a colaborar con cualquiera de ellos o en sus fines. (BOE, 2015)

Este artículo incorporó el delito de adoctrinamiento pasivo, uno de los más debatidos en la doctrina penal contemporánea, por cuanto permite castigar la mera consulta reiterada de contenidos extremistas, sin necesidad de vínculo directo con una organización terrorista. La finalidad de esta formulación es anticipar la intervención penal a las fases más incipientes del proceso de radicalización, especialmente en entornos digitales donde no existen estructuras físicas ni jerarquías claras.

El artículo 577, sanciona diferentes tipologías con relación a la colaboración con organización terrorista, la información o vigilancia sobre personas u objetivos materiales, la prestación de servicios tecnológicos, enaltecimiento, etc., pero sobre todo introduciendo por primera vez la captación de menores o personas especialmente vulnerables con fines terroristas, previendo:

2. [...] Las penas se impondrán en su mitad superior, pudiéndose llegar a la superior en grado, cuando los actos previstos en este apartado se hubieran dirigido a menores de edad o personas con discapacidad necesitadas de especial protección o a mujeres víctimas de trata con el fin de convertirlas en cónyuges, compañeras o esclavas sexuales de los autores del delito, sin perjuicio de imponer las que además procedan por los delitos contra la libertad sexual cometidos. (BOE, 2015)

Este precepto resultó crucial para responder a una realidad alarmante, la seducción y adoctrinamiento terrorista de adolescentes y jóvenes inestables a través de redes sociales, foros, chats cifrados o videojuegos, fenómeno que se había detectado por las FCSE en la “Operación Ghuraba”, y que la Fiscalía de la Audiencia Nacional, expuso de forma ilustrativa en sus memorias relativas al año 2017:

Las D.P. 85/2014. Sumario 6/2015, Operación GHURABA: se trataba de una célula que operaba en Facebook, adoctrinando y captando personas a favor del Estado Islámico. Operación explotada el 13/3/2015, se presentó el escrito de acusación el 14 de septiembre de 2016 y se celebró el juicio oral del 12 al 16 de diciembre de 2016, habiendo resultado condenados todos los acusados. (Fiscalía General del Estado 2027, p.324)

Así mismo, los artículos 578 y 579 relativos al enaltecimiento del terrorismo introducen la realización de estas conductas a través del entorno virtual:

Se castiga el enaltecimiento o justificación públicos del terrorismo, los actos de descrédito, menosprecio o humillación de las víctimas, así como la difusión de mensajes o consignas para incitar a otros a la comisión de delitos de terrorismo. En la tipificación de estas conductas se tiene en especial consideración el supuesto en que se cometan mediante la difusión de servicios o contenidos accesibles al público a través de medios de comunicación, internet, o por medio de servicios de comunicaciones electrónicas o mediante el uso de tecnologías de la información, articulando, además, la posibilidad de que los jueces puedan acordar como medida cautelar la retirada de estos contenidos. (BOE, 2015)

Desde ese momento, nuestro Código Penal permitía sancionar tanto al instructor como al sujeto facilitador que comparte tutoriales, manuales o materiales técnicos yihadistas en canales públicos o privados del ámbito digital, bien sea en foros, Telegram, redes sociales, plataformas de vídeo, etc. Así como al enaltecimiento a través de las mismas vías.

Con esta arquitectura normativa, el legislador español no solo pretendía ampliar el perímetro punitivo, sino construir un sistema de alerta temprana penal que permitiera detectar indicios de radicalización sin necesidad de esperar al atentado. Como señala Silva Sánchez (2020), “la LO 2/2015 consagra definitivamente la lógica del derecho penal de la anticipación, con todas sus potencialidades y riesgos para el principio de intervención mínima” (p. 89).

Por todo ello, la promulgación de la Ley Orgánica 13/2015, de 5 de octubre, de modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica, vino a consolidar el giro estratégico del ordenamiento jurídico español hacia un

modelo procesal adaptado al entorno digital, tecnológicamente competente y capaz de hacer frente a las nuevas lógicas delictivas. Si la LO 2/2015 había reformado el Código Penal en clave de prevención y anticipación frente al terrorismo, la LO 13/2015 vino a completar esa arquitectura legal al modificar profundamente la Ley de Enjuiciamiento Criminal (LECrim), incorporando nuevas figuras, nuevas medidas de investigación y, por primera vez, una regulación expresa del Agente Encubierto Informático o también llamado, Agente Encubierto Virtual.

10.2. EL AGENTE ENCUBIERTO TRADICIONAL

10.2.1. Raíces históricas y práctica de la investigación encubierta en el ordenamiento jurídico español

La necesidad del Estado de observar sin ser visto no es exclusiva de la era contemporánea. En el caso español, el uso de formas rudimentarias de investigación secreta puede rastrearse hasta los primeros cuerpos policiales con funciones de inteligencia interna. En 1824, durante el reinado de Fernando VII, se instituyó la Policía General del Reino y, poco después, se creó el llamado Cuerpo de Policía Secreta, concebido expresamente como instrumento de defensa del régimen absolutista. Este antecedente no solo revela la temprana implantación de prácticas de vigilancia encubierta, sino que demuestra la simbiosis histórica entre poder político y dispositivos de control clandestino (Sánchez, 2022, p. 2).

A lo largo del siglo XIX y principios del XX, España fue desarrollando gradualmente mecanismos informales de infiltración en contextos de disidencia política, especialmente en periodos convulsos como la Restauración o la Dictadura de Primo de Rivera. No obstante, fue durante la Guerra Civil y la posguerra inmediata cuando estos dispositivos de vigilancia adquirieron una dimensión estructural, si bien carente aún de regulación jurídica expresa. Se crearon múltiples servicios de información como el Servicio de Información Militar (SIM), el DEDIDE o el SIDE, orientados a tareas de inteligencia, contraespionaje y sabotaje. Muchos de estos organismos operaban al margen de cualquier control judicial y con escasísima rendición de cuentas pública (Ros, 2016, p. 7; Bertran y Musitu, 1940).

Estas formas tempranas de operaciones encubiertas no eran aun lo que hoy conocemos jurídicamente como tales. Se trataba de misiones secretas de carácter político o militar, ejecutadas por espías, confidentes o diplomáticos, cuyas actuaciones, muchas veces extramuros de la legalidad, eran amparadas por la lógica de la razón de Estado y cuyos archivos, en su mayoría, han sido destruidos o siguen clasificados. Esta opacidad archivística ha dificultado enormemente su estudio, como destaca Sánchez (2022), quien remarca que “de dichas operaciones, dado su carácter secreto, no existen muchas referencias bibliográficas” (p. 3).

Con la consolidación del franquismo tras 1939, la vigilancia encubierta adquirió un sesgo aún más ideológico, con una marcada orientación hacia la represión de la disidencia interna. El Estado recurrió a redes de agentes encubiertos, confidentes y provocadores que, sin cobertura legal, actuaban infiltrados en entornos políticos, religiosos y universitarios. Como antecedente directo del actual agente encubierto, estas figuras compartían su carácter clandestino, su identidad simulada y su proximidad con el delito, pero carecían por completo de las garantías jurídicas que exige el Estado de Derecho. Llegando incluso a permitirles cometer delitos durante el devenir de sus operaciones, tal y como se desprende en la STS 2873/1975 de 14 de junio, que en relación con un suceso expresa: “hechos aparentemente punibles, pero en realidad, causados por el agente provocador de los mismos”, o de similar manera evidenciados en la STS 786/1973 de 20 de febrero.

Si bien, tal y como sostiene Ruíz (1982), “con el paso del tiempo estas investigaciones secretas comenzaron a emplearse en la investigación de los crímenes” (p. 39).

Fue en los años 70 y 80, ante el auge del terrorismo autóctono de España, ETA, GRAPO, FRAP, MPAIAC, etc. y del narcotráfico internacional, cuando se incrementó significativamente el uso de agentes infiltrados en investigaciones penales. Sin embargo, estas actuaciones adolecían de una ausencia total de regulación procesal, lo que generaba un marco de inseguridad jurídica tanto para los agentes como para los encausados.

En palabras del Tribunal Supremo, en su Sentencia 1570/1984, de 15 de noviembre, se reconocía que:

Las fuerzas policiales, como las de la Guardia Civil, tienen, entre otras funciones, las de prevenir el delito, ejerciendo una misión de profilaxis social, y la de descubrir su perpetración, identificando a los autores de las infracciones delictivas, aprehendiéndoles y poniéndolos a disposición judicial; siendo uno de los procedimientos de investigación utilizados al efecto, el de la infiltración, de incógnito y sin revelar su identidad ni su condición pública, en las huestes delictivas o en el medio ambiente o entorno social frecuentado por infractores de la Ley, con el fin de conocer sus planes, de abortarlos, de descubrir a los autores de hechos punibles y de procurar su detención. (STS, 1984)

De esta forma, la tradición jurídica evidencia como en nuestro país se realizaban este tipo de investigaciones encubiertas o de infiltración, bien desde el ámbito militar o el policial. Si bien, este panorama de inseguridad jurídica y vulnerabilidad legal persistió hasta la promulgación de la Ley Orgánica 5/1999, de 13 de enero, que por primera vez reguló formalmente la figura del agente encubierto en el artículo 282 bis de la Ley de Enjuiciamiento Criminal. Este paso marcó el cierre de una etapa de operativos extralegales y el inicio de un modelo de investigación encubierta dotado de respaldo judicial, garantías procesales y exención penal condicionada.

10.2.2. El Agente Encubierto tras la promulgación de la Ley de Enjuiciamiento Criminal de 1999

La Ley Orgánica 5/1999, de 13 de enero, supuso un hito fundamental en el perfeccionamiento del marco procesal penal español frente a los desafíos crecientes del crimen organizado. Hasta entonces, la figura del agente encubierto operaba en un limbo jurídico, apoyada exclusivamente en criterios jurisprudenciales y prácticas policiales que, aunque eficaces, carecían de una cobertura legal explícita. La creciente penetración en España de redes criminales transnacionales dedicadas al narcotráfico, el blanqueo de capitales o el tráfico de armas generó una demanda legislativa urgente de técnicas de investigación más eficaces, pero garantistas. Como afirmaba la Exposición de Motivos de la propia LO 5/1999, se hacía imprescindible “reforzar el aparato judicial frente a organizaciones criminales que, aprovechando las lagunas normativas, operan con un grado de impunidad inaceptable” (BOE, 1999).

Hasta la entrada en vigor de dicha reforma, el agente encubierto era una figura reconocida exclusivamente a través de sentencias del Tribunal Supremo. En este sentido, la STS de 4 de marzo de 1992 ya admitía la validez de actuaciones policiales bajo identidad ficticia siempre que se respetaran los principios de necesidad, legalidad y proporcionalidad. Del mismo modo, la STS de 2 de julio de 1993 consolidó este criterio, subrayando que la actuación encubierta podía ser “válida y legítima siempre que exista un control judicial suficiente que garantice los derechos fundamentales del investigado”. Esta jurisprudencia sentó las bases necesarias para que la L.O 5/1999 (LECrim) incorporara de forma extensa y detalladas los requisitos y funciones del Agente Encubierto mediante la formulación del artículo 282 bis, que literalmente dispone:

1. A los fines previstos en el artículo anterior y cuando se trate de investigaciones que afecten a actividades propias de la delincuencia organizada, el Juez de Instrucción competente o el Ministerio Fiscal dando cuenta inmediata al Juez, podrán autorizar a funcionarios de la Policía Judicial, mediante resolución fundada y teniendo en cuenta su necesidad a

los fines de la investigación, a actuar bajo identidad supuesta y a adquirir y transportar los objetos, efectos e instrumentos del delito y diferir la incautación de los mismos. La identidad supuesta será otorgada por el Ministerio del Interior por el plazo de seis meses prorrogables por períodos de igual duración, quedando legítimamente habilitados para actuar en todo lo relacionado con la investigación concreta y a participar en el tráfico jurídico y social bajo tal identidad.

La resolución por la que se acuerde deberá consignar el nombre verdadero del agente y la identidad supuesta con la que actuará en el caso concreto. La resolución será reservada y deberá conservarse fuera de las actuaciones con la debida seguridad.

La información que vaya obteniendo el agente encubierto deberá ser puesta a la mayor brevedad posible en conocimiento de quien autorizó la investigación. Asimismo, dicha información deberá aportarse al proceso en su integridad y se valorará en conciencia por el órgano judicial competente.

2. Los funcionarios de la Policía Judicial que hubieran actuado en una investigación con identidad falsa de conformidad a lo previsto en el apartado 1, podrán mantener dicha identidad cuando testifiquen en el proceso que pudiera derivarse de los hechos en que hubieran intervenido y

siempre que así se acuerde mediante resolución judicial motivada, siéndole también de aplicación lo previsto en la Ley Orgánica 19/1994, de 23 de diciembre.

Ningún funcionario de la Policía Judicial podrá ser obligado a actuar como agente encubierto.

3. Cuando las actuaciones de investigación puedan afectar a los derechos fundamentales, el agente encubierto deberá solicitar del órgano judicial competente las autorizaciones que, al respecto, establezca la Constitución y la Ley, así como cumplir las demás previsiones legales aplicables.

5. El agente encubierto estará exento de responsabilidad criminal por aquellas actuaciones que sean consecuencia necesaria del desarrollo de la investigación, siempre que guarden la debida proporcionalidad con la finalidad de la misma y no constituyan una provocación al delito.

Para poder proceder penalmente contra el mismo por las actuaciones realizadas a los fines de la investigación, el Juez competente para conocer la causa deberá, tan pronto tenga conocimiento de la actuación de algún agente encubierto en la misma, requerir informe relativo a tal

circunstancia de quien hubiere autorizado la identidad supuesta, en atención al cual resolverá lo que a su criterio proceda. (BOE, 1999)

Así mismo, el punto 4 de dicha Ley, ha sufrido diversas variaciones a través de la Ley orgánica 5/2010 de 22 de Junio, y la Ley Orgánica 15/2003, de 25 noviembre por las que se modificaron la Ley Orgánica 10/1995 de 23 de noviembre, del Código Penal, y que añade los siguientes extremos con relación a la delincuencia organizada y la tipología de delitos en los que se podría instaurar la figura de un Agente Encubierto:

4. A los efectos señalados en el apartado 1 de este artículo, se considerará como delincuencia organizada la asociación de tres o más personas para realizar, de forma permanente o reiterada, conductas que tengan como fin cometer alguno o algunos de los delitos siguientes:

a) Delitos de obtención, tráfico ilícito de órganos humanos y trasplante de los mismos, previstos en el artículo 156 bis del Código Penal.

b) Delito de secuestro de personas previsto en los artículos 164 a 166 del Código Penal.

c) Delito de trata de seres humanos previsto en el artículo 177 bis del Código Penal.

d) Delitos relativos a la prostitución previstos en los artículos 187 a 189 del Código Penal.

e) Delitos contra el patrimonio y contra el orden socioeconómico previstos en los artículos 237, 243, 244, 248 y 301 del Código Penal.

f) Delitos relativos a la propiedad intelectual e industrial previstos en los artículos 270 a 277 del Código Penal.

g) Delitos contra los derechos de los trabajadores previstos en los artículos 312 y 313 del Código Penal.

h) Delitos contra los derechos de los ciudadanos extranjeros previstos en el artículo 318 bis del Código Penal.

i) Delitos de tráfico de especies de flora o fauna amenazada previstos en los artículos 332 y 334 del Código Penal.

j) Delito de tráfico de material nuclear y radiactivo previsto en el artículo 345 del Código Penal.

k) Delitos contra la salud pública previstos en los artículos 368 a 373 del Código Penal.

l) Delitos de falsificación de moneda, previsto en el artículo 386 del Código Penal, y de falsificación de tarjetas de crédito o débito o cheques de viaje, previsto en el artículo 399 bis del Código Penal.

m) Delito de tráfico y depósito de armas, municiones o explosivos previsto en los artículos 566 a 568 del Código Penal.

n) Delitos de terrorismo previstos en los artículos 572 a 578 del Código Penal.

o) Delitos contra el patrimonio histórico previstos en el artículo 2.1.e de la Ley Orgánica 12/1995, de 12 de diciembre, de represión del contrabando. (BOE, 2010)

Esta habilitación confiere una base legal robusta que permite a los cuerpos policiales participar en la dinámica criminal investigada sin incurrir en responsabilidad penal, siempre que se cumplan los principios de necesidad, idoneidad, proporcionalidad y subsidiariedad.

Sin embargo, tal y como podemos apreciar la regulación del agente encubierto incluye una batería de limitaciones orientadas a evitar su desnaturalización. El apartado 5 del artículo 282 bis aclara expresamente que “el agente encubierto estará exento de responsabilidad criminal por aquellas actuaciones que sean consecuencia necesaria del desarrollo de la investigación, siempre que guarden la debida proporcionalidad [...] y no constituyan una provocación al delito”. Esta precisión legislativa impide la confusión con figuras controvertidas como el agente provocador, cuya actuación tal y como se expresa en la STS 427/2013, de 10 de mayo, “injerta el dolo de delinquir en la otra persona, lo cual invalida las pruebas obtenidas”

Tras su regulación, la doctrina jurisprudencial del Tribunal Supremo ha delimitado progresivamente los contornos del agente encubierto. En la STS 1140/2010, de 29 de diciembre, se delimita conceptualmente dicha figura a través del término anglosajón “undercover”, afirmando que:

El término undercover o agente encubierto, se utiliza para designar a los funcionarios de policía que actúan en la clandestinidad, con identidad supuesta y con la finalidad de reprimir o prevenir el delito.

Agente encubierto, en nuestro ordenamiento será el policía judicial, especialmente seleccionado, que bajo identidad supuesta, actúa pasivamente con sujeción a la Ley y bajo el control del Juez, para investigar delitos propios de la delincuencia organizada y de difícil averiguación, cuando han fracasado otros métodos de la investigación o estos sean manifiestamente insuficientes, para su descubrimiento y permite recabar información sobre su estructura y modus operandi, así como obtener pruebas sobre la ejecución de hechos delictivos, debiéndose aclarar que es preciso diferenciar esta figura del funcionario policial que de forma esporádica y aislada y ante un acto delictivo concreto oculta su condición policial para descubrir un delito ya cometido. (STS 1140/2010)

Del mismo modo, en la STS 1570/1984, previa a la reforma, ya se reconocía la legitimidad de infiltraciones bajo identidad falsa siempre que respetaran el marco constitucional (art. 126 CE) y las garantías procesales.

El avance legislativo de 1999 no solo otorga legitimidad jurídica, sino que también consagra al agente encubierto como técnica de investigación estructural. Tal como señala Zafra (2010), “se trata de un instrumento procesal complejo, con enorme potencial probatorio, pero que exige un rigor absoluto en su aplicación para evitar vulneraciones de derechos fundamentales”. La doctrina penal contemporánea ha ido perfilando los requisitos de validez de estas pruebas,

insistiendo en la trazabilidad judicial de todas las decisiones que afectan al encubierto, desde la solicitud de identidad supuesta hasta la presentación de las pruebas en juicio oral.

Uno de los aspectos más controvertidos respecto al uso de agentes encubiertos tras la LO 5/1999 ha sido la delimitación entre actuación legítima y provocación delictiva. El Tribunal Supremo ha desarrollado una doctrina consolidada que busca proteger el núcleo de derechos fundamentales, especialmente el derecho a un proceso con todas las garantías y el derecho a no ser inducido por el Estado a delinquir, estableciendo criterios de proporcionalidad, control judicial previo y exclusión de pruebas ilícitas.

En la STS 1585/2000, de 17 de octubre, se estableció que “la intervención del agente encubierto debe limitarse a la observación, infiltración y obtención de datos sin propiciar la comisión de hechos delictivos”. Este pronunciamiento subrayó que la prueba obtenida con vulneración de derechos fundamentales, sin respeto a los requisitos del artículo 282 bis LECrim, debe considerarse nula ex artículo 11.1 de la Ley Orgánica del Poder Judicial, que advierte que “no surtirán efecto las pruebas obtenidas, directa o indirectamente, violentando los derechos o libertades fundamentales”.

Asimismo, en el contexto del tráfico de drogas, la STS 1671/2004, de 16 de diciembre, abordó el uso de agentes encubiertos en operaciones complejas de narcotráfico internacional. La Sala Segunda consideró legítima la actuación del agente encubierto, al haberse acreditado que este “no indujo al delito, sino que se limitó a integrarse en una red ya activa, documentando los intercambios de información y productos”. Esta sentencia es especialmente ilustrativa porque delimita la frontera entre el agente legalmente habilitado y el denominado “agente provocador”, cuya actividad vicia el procedimiento desde su raíz.

El Tribunal Supremo ha reiterado que, incluso cuando existe autorización judicial, la actuación del agente debe examinarse desde una perspectiva de necesidad, idoneidad y proporcionalidad. La STS 832/2011, de 3 de noviembre, enfatizó que “el control judicial previo y la finalidad legítima de la investigación no excluyen una fiscalización posterior sobre la legalidad de la actuación, especialmente si esta entra en colisión con el principio acusatorio o la presunción de inocencia”.

Estas resoluciones constituyen la columna vertebral de una doctrina restrictiva y garantista, en línea con los postulados del Tribunal Constitucional y del Tribunal Europeo de Derechos Humanos en materia de pruebas obtenidas en entornos de vigilancia encubierta. La doctrina española ha acogido el principio de proporcionalidad como eje estructurante del juicio de constitucionalidad de la intervención encubierta, proyectándose sobre la prueba, la forma de obtención, su impacto procesal y la cadena de custodia.

Sin embargo, la generalización del uso de los entornos virtuales para la comisión del delito, como es el caso de la pornografía infantil y la expansión del terrorismo global, y en particular la del terrorismo de etiología yihadista, que es la que nos ocupa, han exigido un uso cada vez más refinado de la figura del agente encubierto, especialmente en operaciones digitales. Aunque la LO 5/1999 no contemplaba aún la vertiente virtual que más tarde introduciría la LO 13/2015, sus efectos comenzaron a notarse en el terreno judicial con el uso de agentes en contextos de alto riesgo.

La STS 1094/2010, de 30 de noviembre, constituye uno de los precedentes más relevantes en el tratamiento jurisprudencial del agente encubierto en investigaciones sobre terrorismo. En ella, se evaluó la actuación de un agente infiltrado en una célula yihadista con actividades de captación y adoctrinamiento, validando sus pruebas al haberse cumplido estrictamente con la autorización judicial y con el principio de necesidad operativa.

De modo complementario, la STS 1140/2010, de 29 de diciembre, ya citada, profundizó en la doctrina sobre la actuación pasiva y legal del agente. Según el Alto Tribunal, el agente encubierto “actúa pasivamente con sujeción a la Ley y bajo el control del Juez, para investigar delitos propios de la delincuencia organizada y de difícil averiguación, cuando han fracasado otros métodos de la investigación (STS 1140/2010)”. Esta formulación ha sido utilizada por numerosas Audiencias Provinciales y tribunales inferiores para determinar la validez de la prueba testifical y documental aportada por dichos agentes.

Como señala Zafra (2010), “el uso del agente encubierto implica una tensión permanente entre el principio de eficacia en la persecución penal y la preservación de derechos fundamentales, exigiendo un escrutinio judicial constante y riguroso” (p. 102). Esa tensión se incrementa cuando las operaciones afectan a derechos como

el secreto de las comunicaciones, la libertad religiosa o la libertad ideológica, altamente presentes en las tramas de radicalización.

No menos importante es el control sobre la aportación de la prueba. Según la STS 1057/2014, de 5 de enero de 2015, se invalidó parte de la actuación del agente al acreditarse que las grabaciones aportadas no fueron integrales ni mantenían la cadena de custodia, lo que impidió al acusado ejercer su derecho de defensa. En palabras de la Sala, “la prueba encubierta, por su propia naturaleza, exige una diligencia reforzada en su preservación, documentación y contradicción” (STS 1057/2014).

Esta consolidación respondió a una exigencia democrática: dotar de cobertura jurídica a una técnica de investigación extraordinaria, altamente invasiva, pero esencial en un contexto de criminalidad organizada, transnacional y crecientemente sofisticada.

No obstante, esta regulación presentaba importantes vacíos, pues no delimitaba el tipo de delitos investigables, no exigía motivación específica ni previa judicial en todos los casos, y no abordaba aspectos fundamentales como la duración de la infiltración, el alcance de la inmunidad penal del agente o las consecuencias probatorias de su actuación. Por lo que, la jurisprudencia trató de suplir esas lagunas mediante una doctrina restrictiva y garantista, estableciendo, entre otros, que “la autorización judicial resulta imprescindible cuando se va a vulnerar algún derecho fundamental del investigado” (STS 395/2014, de 13 de mayo).

Así, puede afirmarse que el modelo español posterior a 1999 se basa en una arquitectura normativa sólida que mediante el artículo 282 bis de la LECrim, ofrece una doctrina jurisprudencial garantista, y un sistema de control judicial que, aunque mejorable, ha permitido legitimar constitucionalmente la figura del agente encubierto.

10.3. CUERPOS POLICIALES FACULTADOS PARA ERIGIRSE COMO AGENTE ENCUBIERTO

Una vez consolidado el análisis sobre la génesis y regulación normativa del agente encubierto tras la reforma operada por la Ley Orgánica 5/1999, resulta obligado detenerse ahora en la interpretación jurídica del elemento subjetivo habilitante para el ejercicio de esta figura: el sujeto que puede erigirse como tal. En

efecto, el artículo 282 bis de la Ley de Enjuiciamiento Criminal establece que la actuación como agente encubierto solo podrá ser autorizada respecto de un “funcionario de Policía Judicial especialmente seleccionado”. Lejos de constituir una mera fórmula genérica o ambigua, esta expresión remite a un régimen normativo complejo y articulado, que hunde sus raíces en la propia arquitectura constitucional y procesal del Estado de Derecho.

En tal sentido, es imprescindible acudir al marco legal que regula el estatuto, funciones y naturaleza de la Policía Judicial en el ordenamiento español. Dicho marco parte, como no podría ser de otro modo, del artículo 126 de la Constitución Española de 1978, donde se proclama el principio rector de subordinación funcional de la Policía Judicial al Poder Judicial y al Ministerio Fiscal, que expresa: “La Policía Judicial depende de los Jueces, de los Tribunales y del Ministerio Fiscal en sus funciones de averiguación del delito y descubrimiento y aseguramiento del delincuente” (Constitución Española, 1978, art. 126).

Sumado a lo anterior, la facultad para actuar como agente encubierto encuentra su fundamento jurídico en la Ley de Enjuiciamiento Criminal (LECrim), que establece en su artículo 282 de manera clara el objeto y obligación de la policía judicial:

Averiguar los delitos públicos que se cometieren en su territorio o demarcación; practicar, según sus atribuciones, las diligencias necesarias para comprobarlos y descubrir a los delincuentes, y recoger todos los efectos, instrumentos o pruebas del delito de cuya desaparición hubiere peligro, poniéndolos a disposición de la autoridad judicial. (BOE, 2025)

Asimismo, con relación al Agente Encubierto, el artículo 282 bis expone que únicamente los jueces y fiscales, “podrán autorizar a los funcionarios de la policía judicial [...] a actuar bajo identidad supuesta (BOE, 1999)”

Siendo especialmente relevante el artículo 283, que señala expresamente que organismos constituyen la Policía Judicial, cuyo literal expone que:

Constituirán la Policía judicial y serán auxiliares de los Jueces y Tribunales competentes en materia penal y del Ministerio fiscal, quedando obligados a seguir las instrucciones que de aquellas autoridades reciban a efectos de la investigación de los delitos y persecución de los delincuentes:

Primero. Las Autoridades administrativas encargadas de la seguridad pública y de la persecución de todos los delitos o de algunos especiales.

Segundo. Los empleados o subalternos de la policía de seguridad, cualquiera que sea su denominación.

Tercero. Los Alcaldes, Tenientes de Alcalde y Alcaldes de barrio.

Cuarto. Los Jefes, Oficiales e individuos de la Guardia Civil o de cualquier otra fuerza destinada a la persecución de malhechores.

Quinto. Los Serenos, Celadores y cualesquiera otros Agentes municipales de policía urbana o rural.

Sexto. Los Guardas de montes, campos y sembrados, jurados o confirmados por la Administración.

Séptimo. Los funcionarios del Cuerpo especial de Prisiones.

Octavo. Los Agentes judiciales y los subalternos de los Tribunales y Juzgados.

Noveno. El personal dependiente de la Jefatura Central de Tráfico, encargado de la investigación técnica de los accidentes. (BOE,1999)

Finalizando tal argumentario con el artículo 287, que expone que:

Los funcionarios que constituyen la Policía judicial practicarán sin dilación, según sus atribuciones respectivas, las diligencias que los funcionarios del Ministerio fiscal les encomienden para la comprobación del delito y averiguación de los delincuentes y todas las demás que durante el curso de la causa les encargaren los Jueces de instrucción y municipales. (BOE, 1999)

Sin embargo, este marco normativo general es reforzado por la Ley Orgánica 2/1986, de Fuerzas y Cuerpos de Seguridad, que reserva a la Guardia Civil y la Policía Nacional como Fuerzas y Cuerpos de Seguridad del Estado, la competencia plena para integrar unidades de Policía Judicial, legalmente habilitadas por el Ministerio del Interior, tal y como se expone en su preámbulo:

Las Unidades de Policía Judicial son el puente de unión entre las Fuerzas y Cuerpos de Seguridad y el Poder Judicial, es punto central de regulación de aquéllas, el tratamiento de las correspondientes relaciones de dependencia, respecto a Jueces v Fiscales, así como el procedimiento de adscripción de funcionarios o equipo de Policía de dichas Unidades. (BOE, 1986)

Sumado a las anteriores normativas, debemos hacernos eco del Real Decreto 769/1987, sobre la regulación de la Policía Judicial, que en su artículo 1 deja abierta la puerta a otras policías que no sean las estatales, Guardia Civil y Policía Nacional, expresando que:

Las funciones generales de policía judicial corresponden a todos los miembros de las Fuerzas y Cuerpos de Seguridad cualquiera que sea su naturaleza y dependencia, en la medida en que deben prestar la colaboración requerida por la Autoridad Judicial o el Ministerio Fiscal en actuaciones encaminadas a la averiguación de delitos o descubrimiento y aseguramiento de delincuentes, con estricta sujeción al ámbito de sus respectivas competencias, y sin perjuicio de lo dispuesto en el artículo 283 de la Ley de Enjuiciamiento Criminal. (BOE, 1987)

No obstante, un hito importante lo tenemos en la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial, donde en su artículo 547 se amplía el concepto de Policía Judicial “a todos los miembros de las Fuerzas y Cuerpos de Seguridad, tanto si dependen del Gobierno central como de las comunidades autónomas o de los entes locales, dentro del ámbito de sus respectivas competencias” (BOE, 2004).

Contexto que evidencia como, tanto los Mossos d'Esquadra (Cataluña), como la Ertzaintza (País Vasco) y la Policía Foral de Navarra pueden ejercer como agentes encubiertos, siempre que estén integrados formalmente en unidades de Policía Judicial.

10.3.1. La Policía autonómica catalana, los Mossos d'Esquadra como Policía Judicial

El Cuerpo de Mossos d'Esquadra representa, por evolución histórica y por desarrollo legislativo, la policía integral de Cataluña con plenas competencias en el ámbito de la seguridad pública, incluyendo la función de Policía Judicial. Esta habilitación normativa, además de tener sustento estatutario, ha sido consolidada mediante legislación autonómica y estatal, así como a través de diversos convenios de colaboración entre la Generalitat de Cataluña y el Estado.

El punto de partida normativo se encuentra en el Estatuto de Autonomía de Cataluña, aprobado por la Ley Orgánica 6/2006, de 19 de julio, de reforma del Estatuto de Autonomía de Cataluña, en su artículo 1º le transfiere a la Generalitat “la creación de la policía de la Generalitat-Mossos d'Esquadra”. Estableciendo en su artículo 164 las funciones de Seguridad pública que les corresponden a dicho cuerpo policial:

La Policía de la Generalitat-Mossos d'Esquadra tiene como ámbito de actuación el conjunto del territorio de Cataluña y ejerce todas las funciones propias de un cuerpo de policía, en los siguientes ámbitos:

- a) La seguridad ciudadana y el orden público.
- b) La policía administrativa, que incluye la que deriva de la normativa estatal.
- c) La policía judicial y la investigación criminal, incluidas las diversas formas de crimen organizado y terrorismo, en los términos establecidos por las leyes. (BOE, 2006)

Este mandato estatutario se desarrolla en la Ley 10/1994, de 11 de julio, de la Policía de la Generalitat-Mossos d'Esquadra, norma que regula en profundidad su actuación como policía judicial. En su exposición de motivos, se afirma que:

El Cuerpo de Mossos d'Esquadra actuará, en funciones de policía judicial, en los términos establecidos por los artículos 126 de la Constitución, 13.5 del Estatuto de autonomía y 443 y siguientes de la Ley Orgánica del Poder Judicial.

El auxilio a jueces, tribunales y fiscales en la investigación de los delitos y en la identificación y detención de los delincuentes, ya sea a requerimiento ajeno o por iniciativa propia, constituye una actividad esencial, prioritaria y permanente de cualquier policía. Por esta razón, el Cuerpo de «Mossos d'Esquadra» prevé la creación de unidades especiales de policía judicial, formando a los correspondientes funcionarios, para adscribirlas a los citados órganos jurisdiccionales y al Ministerio Fiscal.
(BOE, 1994)

Estipulando, además:

El Cuerpo de Mossos d'Esquadra, como policía ordinaria e integral, ejerce las funciones que el ordenamiento jurídico atribuye a las Fuerzas y Cuerpos de Seguridad, y, en concreto: funciones de seguridad ciudadana, funciones de policía administrativa, y las funciones de policía judicial que le correspondan de acuerdo con el artículo 13.5 del Estatuto de autonomía,

y que se establecen en el artículo 126 de la Constitución Española, los artículos 443 y 445 de la Ley Orgánica del Poder Judicial y el resto de la legislación procesal vigente. (BOE, 1994)

De esta manera, si bien el artículo 282 bis LECrim no menciona expresamente a los Mossos d'Esquadra, el conjunto de normas que regula la función de Policía Judicial incluye a los cuerpos autonómicos, siempre que actúen dentro de su competencia territorial, funcional y bajo la supervisión judicial o del Ministerio Fiscal.

En este sentido, la STS 1140/2010, de 29 de diciembre, ratifica que el agente encubierto debe actuar bajo identidad supuesta, con autorización judicial y controlado judicialmente, sin que ello excluya por principio a los cuerpos autonómicos legalmente habilitados como policías judiciales.

10.3.2. La Policía autonómica vasca, la Ertzaintza como Policía Judicial

El punto de partida para acreditar la competencia de la Ertzaintza como cuerpo facultado para actuar como Policía Judicial y, por tanto, susceptible de asumir funciones como Agente Encubierto bajo el artículo 282 bis LECrim, se encuentra en el propio Estatuto de Autonomía del País Vasco, aprobado mediante Ley Orgánica 3/1979, de 18 de diciembre. En su artículo 17 se reconoce expresamente que “corresponderá a las Instituciones del País Vasco, en la forma que se determina en este Estatuto, el régimen de la Policía Autónoma para la protección de las personas y bienes y el mantenimiento del orden público dentro del territorio autónomo” (BOE,1979).

Este marco competencial se amplía y concreta con el Decreto Legislativo 1/2020, de 29 de julio, por el que se aprueba el Texto Refundido de la Ley de Policía del País Vasco, norma autonómica que regula el funcionamiento de la Ertzaintza, que en su artículo 50 les otorga competencias de policía judicial:

1. Compete a todos los funcionarios y funcionarias de la Ertzaintza el

auxilio en la averiguación de los delitos y en el descubrimiento y

aseguramiento de delincuentes, como Policía judicial, en el ámbito de sus competencias definidas en el artículo 17 del Estatuto de Autonomía y los acuerdos de delimitación de funciones suscritos por la Junta de Seguridad, sin menoscabo de las funciones de dirección de las autoridades judiciales y el Ministerio Fiscal.

2. En la estructura de la Ertzaintza se establecerán unidades de investigación criminal y Policía judicial que dependerán funcionalmente de las autoridades judiciales y del Ministerio Fiscal en el desempeño de todas las actuaciones que aquellas les encomienden contempladas en la Ley Orgánica del Poder Judicial. Quienes ostenten la responsabilidad de tales unidades policiales serán responsables de canalizar los requerimientos provenientes de las autoridades judiciales y del Ministerio Fiscal, a los efectos de que el personal o medios de las referidas unidades intervengan en una investigación. (BOE, 2020)

Equiparándolos su artículo 52 con las mismas atribuciones que las FCSE en su relación con las autoridades judiciales, exponiendo su punto tercero que:

Los órganos judiciales de la jurisdicción penal y el Ministerio Fiscal tendrán, respecto de las unidades de investigación criminal y Policía judicial que les sean adscritos con carácter permanente, las mismas

facultades que les reconoce el artículo 35 de la Ley Orgánica 2/1986, de 13 de marzo, de Fuerzas y Cuerpos de Seguridad. (BOE, 2020)

Reflejando su artículo 23, que durante su desempeño como policía judicial, deberán en todo momento respetar la autoridad de los tribunales y prestarán su servicio bajo la “dependencia de la Administración de justicia, en los términos que dispongan las leyes” (BOE, 2020).

Esta disposición satisface el requisito que impone el artículo 282 bis de la LECrim, que exige que el agente encubierto sea un “funcionario de la Policía Judicial especialmente seleccionado” (BOE, 1999). La ley vasca asegura tanto el carácter de policía judicial como la especialización profesional del agente, que sumado a lo establecido en el artículo 547 de la Ley Orgánica del Poder Judicial, no cabe objeción legal alguna a que un miembro de la Ertzaintza sea autorizado judicialmente para operar como Agente Encubierto.

10.3.3. La Policía Foral de Navarra como Policía Judicial

Al igual que los Mossos y la Ertzaintza, la habilitación de la Policía Foral de Navarra para ejercer funciones de Policía Judicial deriva de una combinación de fuentes normativas estatales y forales, que en conjunto consolidan su legitimación dentro del marco del artículo 282 bis de la Ley de Enjuiciamiento Criminal.

En primer lugar, el Estatuto de Autonomía de Navarra articulado en la Ley Orgánica 13/1982, de 10 de agosto, de reintegración y mejoramiento del Régimen Foral de Navarra, establece en su artículo 51 que: “corresponde a Navarra la regulación del régimen de la Policía Foral que, bajo el mando supremo de la Diputación Foral, continuará ejerciendo las funciones que actualmente ostenta” (BOE, 1982).

Sobre esta base, Navarra desarrolló su propio cuerpo policial, la Policía Foral, dotándole de funciones plenas en materia de seguridad, entre ellas, las que derivan de la investigación criminal bajo la autoridad judicial; consolidándose a través de la Ley Foral 8/2007, de 23 de marzo, reguló la Policía Foral de Navarra, que posteriormente fue actualizada a su última norma Ley Foral 23/2018, de 19 de

noviembre, de las policías de Navarra, que en su artículo 2 destaca entre las finalidades de dicha policía, la protección por los derechos y libertades que establece el ordenamiento jurídico, el respeto a la ley, así como luchar contra la delincuencia (BOE, 2018).

Más adelante, el artículo 16 establece las funciones que ejercerá dicho cuerpo de seguridad, entre las que se destacan las de “policía Judicial”, pasando a especificar tales funciones en el artículo 19, que expone:

1. La Policía Foral de Navarra ejercerá las funciones generales de Policía Judicial que le atribuye el ordenamiento jurídico y prestará, a través de los cauces pertinentes, la colaboración requerida por la autoridad judicial o el Ministerio Fiscal en actuaciones encaminadas a investigar y perseguir los delitos para descubrir y detener a los presuntos culpables, asegurar los instrumentos, efectos y pruebas del delito, poniéndolos a disposición del Juez o Tribunal competente, y elaborar los informes técnicos y periciales procedentes.

2. A efectos de lo dispuesto en el apartado anterior, reglamentariamente se establecerán, dentro de la estructura orgánica de la Policía Foral de Navarra, unidades con funciones de Policía Judicial, que podrán adscribirse a determinados Juzgados o Tribunales o al Ministerio Fiscal.

4. El personal adscrito a las unidades de Policía Judicial dependerá funcionalmente de los Jueces y Tribunales o del Ministerio Fiscal que estén conociendo del asunto objeto de su investigación. (BOE, 2018)

Asimismo, con relación a la Ley Orgánica 2/86 de Fuerzas y Cuerpos de Seguridad, el artículo 23 otorga a las policías locales de Navarra todas las funciones atribuidas por dicha ley, y en particular, las funciones de “policía judicial en los casos y formas que señale la legislación vigente” (BOE, 2018), que se complementan con el artículo 547 de la Ley Orgánica del Poder Judicial. En consecuencia, todo ello satisface sin ambigüedad alguna, el requisito legal que exige el artículo 282 bis de la LECrim al referirse a que sólo podrán ejercer como Agentes encubiertos los funcionarios de la policía judicial, respondiendo como la Policía Foral de Navarra es a todas luces una unidad de Policía Judicial.

10.3.4. El Servicio de Vigilancia Aduanera como Policía Judicial

En primer lugar, conviene subrayar que el SVA sí tiene reconocida la condición de policía judicial en el ordenamiento jurídico español. Este reconocimiento se fundamenta en los siguientes preceptos:

Artículo 283.4 de la LECrim, al enumerar los cuerpos auxiliares de jueces y fiscales en funciones de policía judicial, incluye “cualquier otra fuerza destinada a la persecución de malhechores”, categoría en la que ha sido subsumido el SVA por la doctrina y la jurisprudencia.

Ley Orgánica 6/1985, del Poder Judicial, en su artículo 547 señala que “todos los miembros de las Fuerzas y Cuerpos de Seguridad, tanto si dependen del Gobierno central como de las comunidades autónomas o de los entes locales”, pueden ejercer funciones de policía judicial dentro de sus respectivas competencias. Aunque el SVA no se integra expresamente en las Fuerzas y Cuerpos de Seguridad, su consideración funcional como auxiliar de la justicia penal ha sido respaldada por la jurisprudencia.

Real Decreto 769/1987, que regula las Unidades de Policía Judicial, señala en su artículo 1 que las funciones generales de policía judicial “corresponden a todos los miembros de las Fuerzas y Cuerpos de Seguridad, cualquiera que sea su naturaleza y dependencia [...] con estricta sujeción al ámbito de sus respectivas competencias” (BOE, 1987). En consecuencia, el SVA puede ejercer funciones investigadoras y colaboradoras bajo dirección judicial en el ámbito de los delitos económicos.

La STS 1293/2005, de 14 de noviembre, reconoce expresamente la actuación del SVA como auxiliar del juez instructor en calidad de policía judicial, y valida diligencias por él instruidas con plenos efectos procesales. En este sentido, se ha dicho que el SVA “actúa como policía judicial especializada en delitos económicos y aduaneros” siempre que opere bajo control jurisdiccional.

No obstante, ser policía judicial no implica automáticamente estar habilitado para ejercer como agente encubierto bajo el régimen del artículo 282 bis LECrim, que exige “autorización judicial o del Ministerio Fiscal para que funcionarios de la Policía Judicial actúen bajo identidad supuesta” (BOE, 1999).

Aquí es donde se genera la controversia en torno al SVA; si bien puede actuar como policía judicial, no pertenece formalmente a las Fuerzas y Cuerpos de Seguridad del Estado, ni a los cuerpos autonómicos reconocidos, y por tanto no ha sido tradicionalmente considerado habilitado para asumir el rol de agente encubierto en operaciones con identidad falsa o en infiltración.

En esta línea, la jurisprudencia ha sido cautelosa. Pues, no existe a día de hoy doctrina consolidada del Tribunal Supremo que reconozca al SVA la facultad de actuar como agente encubierto con plena legitimidad en el sentido del art. 282 bis LECrim. En los casos en que ha participado en operaciones complejas, como las relacionadas con el blanqueo de capitales o el contrabando, su rol se ha limitado al de colaborador técnico y ejecutor de diligencias de investigación, sin poder adoptar identidad supuesta.

La STS 1097/2002, de 5 de junio y la STS 275/2007, de 28 de marzo, confirman que la legitimación del agente encubierto exige un acto formal de habilitación por parte del juez o fiscal y que el agente pertenezca a una fuerza policial reconocida, con formación específica. En ellas, se sugiere que solo cuerpos que cuenten con estructuras organizativas específicas para tales operaciones pueden asegurar la legalidad y eficacia de las mismas.

XI – EL AGENTE ENCUBIERTO INFORMÁTICO

XI -EL AGENTE ENCUBIERTO INFORMÁTICO

11.1. EVOLUCIÓN DEL PARADIGMA CRIMINAL EN LA ERA DIGITAL

El sociólogo Castells (2005) ya advertía hace casi dos décadas que “la sociedad red es el paradigma tecnológico de nuestro tiempo, un naciente universo digital que se encuentra en permanente transformación y que se retroalimenta, a la vez que incide directa o indirectamente en la vida de millones de personas” (p. 23). Esta afirmación, más que una tesis teórica, se ha consolidado como una realidad sociológica incuestionable, pues la digitalización ha alterado radicalmente no solo los modos de interacción humana, sino también la propia naturaleza delictiva.

En efecto, la irrupción masiva de internet, las redes sociales, la Dark Web y los foros opacos, junto con los sistemas de mensajería cifrada como Telegram, que se han convertido en la cuna del cibercrimen han modificado de forma sustancial el ecosistema criminal contemporáneo. Ya no se trata de delincuentes que operan en la clandestinidad física o de estructuras organizadas ancladas a un territorio concreto, sino de redes dispersas, ágiles, fluidas y en muchas ocasiones invisibles para el derecho penal tradicional. La criminalidad ha adquirido una dimensión “líquida”, en palabras de Bauman (2000), donde la huella digital sustituye a la evidencia material, y el anonimato en la red plantea desafíos inéditos para la persecución y acreditación del delito.

Esta transformación no solo ha generado nuevas tipologías delictivas como el phishing y el fraude digital, la suplantación de identidad o los deepfakes alimentados por la Inteligencia Artificial, las formas de extorsión por ransomware, las brechas de datos personales que se venden por doquier en foros underground y las amenazas híbridas de actores Estado hostiles; sino que ha requerido de una profunda reconfiguración de las herramientas investigativas del Estado. La criminalidad se ha digitalizado y adaptado de manera sobresaliente al nuevo entorno como si de un campo de batalla a conquistar se tratase, y con ello, el Estado de Derecho ha debido afrontar una disyuntiva crucial: adaptar sus instrumentos normativos al nuevo terreno de juego o resignarse a la impotencia jurídica. Por desgracia, en el ámbito europeo, pese a los avances, nos enfrentamos a criminales

del siglo XXI con herramientas del siglo XX, en tribunales contruidos bajo paradigmas del siglo XIX (Chiara, 2024).

Ante este escenario, emerge con claridad la necesidad de figuras procesales innovadoras que permitan actuar eficazmente en el ciberespacio sin quebrantar las garantías constitucionales. En este sentido, la figura del agente encubierto informático (AEI) surge no como un capricho legislativo, sino como una respuesta jurídico-operativa imprescindible frente a una criminalidad que, si bien intangible, produce consecuencias materiales devastadoras.

En los últimos años, tanto el Tribunal Supremo como la Audiencia Nacional han reconocido el valor estratégico del entorno digital en múltiples resoluciones, especialmente en delitos de terrorismo, corrupción de menores y crimen organizado. Ya en la Sentencia de la Sala Penal del Tribunal Supremo 489/2020, se afirmaba que “el ámbito virtual se ha convertido en un espacio idóneo para la gestación, desarrollo y ejecución de conductas delictivas especialmente graves [...] que exige un esfuerzo hermenéutico para garantizar la eficacia investigadora sin erosionar derechos fundamentales”.

La dificultad reside, sin embargo, en hallar un equilibrio operativo entre la eficacia investigadora y la tutela de derechos como el secreto de las comunicaciones (art. 18.3 CE), la intimidad (art. 18.1 CE) o la presunción de inocencia (art. 24.2 CE). El legislador no puede ceder ante el vértigo tecnológico sin trazar límites precisos, como tampoco puede permitir que la criminalidad digital campe a sus anchas por falta de instrumentos adecuados.

La sociedad de la información ha multiplicado las oportunidades de desarrollo humano, pero también ha dado lugar a nuevas formas de vulnerabilidad. Como recuerda el criminólogo Garland (2001), “las transformaciones estructurales de la modernidad tardía han erosionado las certezas del sistema penal clásico, exigiendo nuevas formas de gobernabilidad frente al riesgo” (p. 48). En este marco de incertidumbre, el derecho penal no puede permanecer inerte, y debe reinventarse sin traicionar sus principios fundacionales.

Por todo ello, los antecedentes de la figura del AEI no pueden entenderse sin partir de este proceso de mutación del crimen, de la tecnología y del propio Estado de Derecho. La lucha contra el delito en el siglo XXI exige no solo nuevas leyes, sino nuevas formas de presencia del Estado allí donde el delito se esconde, bien sean

tras el anonimato de un perfil falso en la red, un foro underground en la dark web, o a través de sistemas de mensajería cifrados como Telegram.

Frente a la constatación de que el delito se ha globalizado y digitalizado, las respuestas jurídicas de corte nacional comenzaron a revelarse insuficientes. La delincuencia informática, por su propia naturaleza transfronteriza y descentralizada, desborda las competencias de los Estados y exige esquemas de colaboración internacional sólidos, ágiles y jurídicamente vinculantes. En ese contexto, el Convenio sobre la Ciberdelincuencia del Consejo de Europa, adoptado en Budapest en 2001, se erige como el primer instrumento internacional vinculante destinado a hacer frente a los delitos cometidos a través de sistemas informáticos y redes digitales.

Este tratado, más conocido como Convenio de Budapest, supuso un punto de inflexión normativo. Tal como recoge el propio preámbulo, su finalidad es “la protección de la sociedad contra la ciberdelincuencia mediante la adopción de una política penal común, la mejora de las técnicas de investigación y la intensificación de la cooperación internacional” (Consejo de Europa, 2001). Así pues, lejos de ser un simple protocolo técnico, el convenio es un documento vivo para combatir estas novedosas formas de criminalidad, y plantea una arquitectura legal que conjuga armonización normativa, herramientas procesales eficaces y una decidida apuesta por la cooperación transfronteriza. Tal y como se expresa en el mismo, sus objetivos son: “prevenir los actos que pongan en peligro la confidencialidad, la integridad y la disponibilidad de los sistemas, redes y datos informáticos, así como el abuso de dichos sistemas, redes y datos, garantizando su tipificación como delito” (Consejo de Europa, 2001); favoreciendo la asunción de un marco legal integral y de cooperación común con el que poder hacer frente de forma satisfactoria a la “detección, investigación y sanción” de los ciberdelitos, junto al desarrollo de novedosas formas de salvaguarda y evidencia electrónica, garantes procesales de los diferentes indicios y pruebas virtuales que se obtengan (Consejo de Europa, 2001).

Para ello, este convenio, prevé una reglamentación que, bajo el principio de proporcionalidad, en connivencia a una estricta supervisión judicial y limitación del ámbito de aplicación y duración de las medidas que procedan, garantice los

derechos humanos y libertades de los ciudadanos en base a tres pilares fundamentales:

1. La criminalización de conductas informáticas específicas, como el acceso ilícito, la interceptación ilegal, la interferencia en datos y sistemas, el uso indebido de dispositivos, el fraude informático y los delitos relacionados con contenidos, como la pornografía infantil.
2. La regulación de medios de prueba y evidencias electrónicas, técnicas de investigación adaptadas al entorno digital y las nuevas formas del cibercrimen, así como el registro remoto de sistemas, la conservación rápida de datos y la obtención de información en tiempo real.
3. El fomento de la cooperación internacional mediante asistencia jurídica mutua, intercambio de datos y estandarización de procedimientos entre autoridades competentes (Consejo de Europa, 2001, arts. 14–35).

No obstante, el éxito del convenio ha dependido de su ratificación e implementación efectiva en los ordenamientos nacionales. En este sentido, no todos los países han reaccionado con igual celeridad ni compromiso. España lo firmó en 2001, pero no lo ratificó hasta septiembre de 2010 (BOE, 2010), entrando en vigor a finales de ese año. Esta demora se explica, en parte, por la complejidad técnica y jurídica de adaptar un marco normativo decimonónico, como el de la Ley de Enjuiciamiento Criminal española (1882), a una realidad digital vertiginosa y cambiante.

Aun ratificado, su aplicación efectiva encontró obstáculos iniciales. Ejemplo paradigmático de ello fue el caso Anonymous–WikiLeaks, que reveló grietas en el aparato legal frente a fenómenos inéditos como el hacktivismo. La campaña de ciberataques lanzada en 2010 por colectivos vinculados a Anonymous, en respuesta a la presión contra Julian Assange y WikiLeaks, afectó gravemente a empresas como Amazon, PayPal, Visa o Mastercard, así como a instituciones públicas (Quintana y Tascón, 2012). Los atacantes utilizaron técnicas de denegación de servicio distribuido (DDoS), saturando servidores mediante cientos de miles de peticiones coordinadas de conexión a dichos servicios, lo que colapsó servicios estratégicos y dejó al descubierto la fragilidad del sistema ante agresiones de nueva generación.

Estas acciones marcaron un antes y un después en la percepción del ciberespacio como zona de riesgo político-criminal. Como apunta Pras et al. (2010),

“el caso Anonymous supuso un punto de inflexión jurídico, en tanto desbordó los marcos clásicos de la criminalidad organizada y evidenció la necesidad de una regulación específica del ciberactivismo y sus límites” (p. 142).

En consecuencia, el Convenio de Budapest no solo inspiró reformas normativas, sino que introdujo un nuevo lenguaje jurídico a través de conceptos como "evidencia digital", "registro remoto", "atribución" o "jurisdicción múltiple" que comenzaron a permear el discurso procesal penal. Aun así, el desfase entre realidad tecnológica y norma positiva persistió durante años, obligando a jueces y fiscales a forzar interpretaciones creativas o a operar en el borde de lo que estipulaba la legislación.

Con todo, el Convenio ha sido decisivo para configurar una gramática penal común sobre la ciberdelincuencia. Como afirma López-Muñoz (2020), “más que un tratado, Budapest es una metodología legal viva que ha permitido construir un sistema internacional de protección de datos, infraestructuras críticas y derechos digitales con vocación armonizadora” (p. 97).

A la luz de estos desarrollos, resultaba inevitable que España reformulara sus categorías jurídicas, especialmente en el terreno de la investigación criminal. Las figuras del agente encubierto clásico, del registro domiciliario, las observaciones telefónicas o del acceso físico a pruebas, comenzaban a resultar obsoletas en un mundo donde el crimen se disfraza de avatar, se oculta tras un cifrado de extremo a extremo, cambia su IP a través de un servicio de red Privada Virtual (VPN) o se disuelve en un servidor remoto fuera del país. Y, es en ese vacío operativo y normativo, donde empezaría a fraguarse la figura del agente encubierto informático, como veremos a lo largo de este capítulo.

En el caso del Estado español, esta validación del convenio marcó el inicio de una transformación jurídica que se tornaba urgente. La ratificación del tratado en 2010 coincidió con una serie de reformas legales que buscaban dotar al sistema penal de herramientas adecuadas para hacer frente al desafío de la ciberdelincuencia. En este contexto, se promulgó la Ley Orgánica 5/2010, de 22 de junio, que introdujo importantes modificaciones al Código Penal de 1995, adaptando tipos delictivos ya existentes como las estafas y daños informáticos y

creando otros nuevos para responder a las amenazas emergentes en el entorno digital (BOE, 2010).

La entrada en vigor de esta norma tuvo una rápida aplicación práctica. El 10 de junio de 2011, las autoridades españolas detuvieron a tres personas identificadas como presuntos responsables de liderar la estructura de Anonymous en territorio nacional. Se les imputó la ejecución de la llamada “Operación Spanish Revolution”, un conjunto de ciberataques dirigidos contra infraestructuras digitales españolas con la intención de mermar la normal celebración de las elecciones municipales y autonómicas que se celebrarían en España el 22 de mayo del 2011. Fruto de dicho ataque, se vio afectada la infraestructura digital de la Junta Electoral Central, el Congreso de los Diputados, la Unión General de Trabajadores y varios partidos políticos mayoritarios. Según los atestados policiales, los ataques se habrían realizado mediante el envío masivo de más de 340.000 correos electrónicos, generando un colapso en los servidores mediante técnicas de denegación de servicio distribuido (DDoS) (Quintana y Tascón, 2012).

Lo relevante del caso, según el Magistrado-Juez del Juzgado Central de Instrucción nº 5 de la Audiencia Nacional, D. José de la Mata, no solo residía en la magnitud de los daños causados, sino en la intervención de un agente encubierto bajo la identidad digital de “*Sprocket*”, cuya actuación suscitó un intenso debate procesal (De la Mata, 2017). La defensa de los acusados alegó que dicho agente habría entablado contacto sin autorización judicial previa, y que su comportamiento podría haber incurrido en una provocación al delito, vulnerando así derechos fundamentales, como el derecho al proceso con todas las garantías (art. 24 CE) y la legalidad de la obtención de pruebas (Quintana y Tascón, 2012).

La sentencia de instancia fue recurrida, y en 2016 se dictó un fallo que absolvía a los acusados de los principales cargos. Si bien se reconoció su participación en los hechos, el tribunal estimó que se habían producido irregularidades en la cadena de custodia de los dispositivos intervenidos, así como ambigüedades en la figura del agente encubierto actuante. No obstante, el juzgado reconoció que, una vez detectada la conducta delictiva en foros y chats públicos, la Policía solicitó de forma diligente la autorización judicial para otorgar a “*Sprocket*” la condición de agente encubierto, amparándose en el artículo 282 bis de la Ley de Enjuiciamiento Criminal.

Este caso, sin duda pionero, evidenció dos grandes carencias: por un lado, la falta de protocolos unificados sobre cómo debe actuar un agente encubierto en entornos digitales; y por otro, la necesidad de reformar en profundidad una Ley de Enjuiciamiento Criminal que databa de 1882 y que apenas había sido tocada desde su última gran reforma en 1999.

Paralelamente a ello, entre los años 2010 y 2012, el norte de África y Oriente Próximo fueron escenario de un proceso de agitación sociopolítica sin precedentes conocido como las “*primaveras árabes*”. Millones de ciudadanos salieron a las calles en países como Túnez, Egipto, Libia, Yemen o Siria reclamando el fin de regímenes autoritarios y la instauración de sistemas democráticos más respetuosos con los derechos humanos. Sin embargo, lo que en principio fue percibido como una oportunidad para el cambio político degeneró, en muchos casos, en caos, guerras civiles y vacío de poder. Este desorden estructural fue rápidamente aprovechado por actores islamistas radicales de corte salafista-yihadista, que supieron instrumentalizar la inestabilidad para sus propios fines.

Aprovechando el desmoronamiento de los aparatos estatales tradicionales, organizaciones terroristas como Al Qaeda en la Península Arábiga (AQPA) o el entonces denominado Estado Islámico de Irak, génesis del Daesh, comenzaron a reclutar, adoctrinar y organizarse en el nuevo escenario, recurriendo de manera intensiva a las nuevas tecnologías de la información y a las redes sociales. La capacidad de estos grupos para entender y dominar el lenguaje digital fue clave para su expansión. Según el analista Vidino (2015), “la revolución yihadista no se libró ya solo en los desiertos de Siria o en las montañas de Afganistán, sino en foros encriptados, canales de Telegram y vídeos virales de Twitter y YouTube” (p. 114).

La gran inflexión se produjo en junio de 2014, cuando Abu Bakr Al Baghdadi proclamó en Mosul el establecimiento del Califato Islámico, dando lugar al fenómeno conocido como Daesh (*Ad-Dawla al-Islamiyya fi al-‘Iraq wa al-Sham*). A partir de ese momento, el uso de internet dejó de ser accesorio para convertirse en elemento estructural del proyecto yihadista global. Se crearon medios de comunicación propios como Al Hayat Media Center, Al-Furqan o Al-Amaq, que difundían sermones cargados de odio e iconoclasia yihadista, manifiestos, manuales tácticos y hasta vídeos con ejecuciones, editados con calidad

cinematográfica. La estética visual se profesionalizó, y con ella la capacidad de captación emocional.

Como subrayó Lesaca (2017), “Daesh desarrolló una narrativa transmedia que apelaba no solo a la dimensión religiosa del combatiente, sino también a su deseo de heroicidad, aventura y pertenencia a una causa trascendente (p. 87).” Esta narrativa permitió a los grupos yihadistas acercarse a jóvenes de todo el mundo, especialmente occidentales, utilizando los códigos culturales del siglo XXI: estética de videojuego, efectos visuales, música épica, retórica sobre el martirio, confrontación de civilizaciones, etc.

Los procesos de adoctrinamiento y captación dejaron de requerir contacto físico. El ciberespacio se convirtió en el nuevo campo de batalla. A través de cuentas falsas, bots, foros cerrados o enlaces efímeros, se creaba un itinerario de radicalización gradual en el que el individuo pasaba de la curiosidad al compromiso en cuestión de semanas. Como recogió la Sentencia de la Audiencia Nacional 21/2014, de 29 de mayo, “la propaganda yihadista en internet se ha convertido en el principal canal de reclutamiento de combatientes, transmitiendo instrucciones tácticas, justificando la violencia e identificando objetivos legítimos de ataque”.

Este modelo de expansión fue particularmente eficaz en Europa. Entre 2013 y 2017, más de 5.000 europeos abandonaron sus países para integrarse en Daesh, de los cuales aproximadamente 1.200 eran residentes en Francia, 800 en Alemania y alrededor de 200 en España, según datos del Centro Internacional para el Estudio de la Radicalización (ICSR, 2018). Muchos de ellos no provenían de entornos religiosos ni de comunidades tradicionales, sino que habían sido captados exclusivamente en línea, a menudo tras procesos de socialización secundaria marcados por la exclusión, la desafección y la búsqueda de sentido vital.

El caso de Mustafá Maya Amaya representa un punto de inflexión en la lucha contra la radicalización yihadista en España. Este ciudadano español, de origen belga y convertido al islam, fue arrestado en Melilla en marzo de 2014 acusado de dirigir una compleja red de captación y envío de combatientes yihadistas a Siria, Libia y Mali. Su actividad, según detalló la Policía Nacional, no se centraba en acciones violentas directas, sino en una labor sostenida de adoctrinamiento digital, promesas de redención religiosa y exaltación de la violencia como mandato divino (Rodríguez, 2014).

Lo significativo de este caso fue que Mustafá Maya no necesitó salir de su domicilio ni reunirse físicamente con sus contactos. Bastaba su conexión a internet para extender su influencia. Desde un pequeño piso de la Cañada de Hidum, en Melilla, operaba como un predicador virtual que utilizaba Facebook, Skype y otros canales para reclutar jóvenes de múltiples nacionalidades: marroquíes, franceses, turcos, belgas, y también españoles. Según la información publicada por El País (Rodríguez, 2014), se le consideró el “mayor captador de yihadistas en territorio nacional”, facilitando la salida de más de una decena de individuos hacia zonas de combate.

Lo más alarmante fue su habilidad para seducir tanto a musulmanes practicantes como a conversos recientes, adaptando su discurso a las inseguridades, frustraciones o anhelos de cada interlocutor. Esta personalización del proceso captador evidencia una dinámica de radicalización psicológicamente sofisticada, imposible de identificar sin vigilancia activa en el entorno digital. Como destaca Reinares (2015), “Maya Amaya demostró que un solo individuo, con los conocimientos y herramientas adecuados, podía tejer desde la penumbra una red de radicalización con proyección internacional” (p. 163).

Esto evidenciaba, que la figura del yihadista no responde ya al arquetipo del combatiente curtido en escenarios bélicos de Afganistán o Chechenia, sino que adopta formas insospechadas en contextos plenamente occidentales. Uno de los ejemplos paradigmáticos es el de Nabil Benkaddour, ciudadano español de origen marroquí, detenido en 2014 en San Pedro del Pinatar (Murcia), cuando intentaba viajar a Siria para unirse a Daesh tras haber jurado lealtad a Abu Bakr al-Baghdadi. Benkaddour, fue captado por medios digitales, principalmente a través de vídeos propagandísticos y sermones difundidos en plataformas cerradas, constatándose por parte de la Guardia Civil como este individuo mantenía:

Una intensa actividad como usuario en foros yihadistas radicales, así como que administraba diferentes perfiles en Facebook y Twitter en los que difundía contenido claramente laudatorio y propagandístico de las ideas y

actividades violentas relacionadas con las organizaciones terroristas de carácter yihadista. (La Verdad/Efe, 2015)

Su perfil, alejado de círculos tradicionales de militancia islamista, representa una de las mutaciones más complejas de la amenaza yihadista: la radicalización autodidacta y emocional, motivada por elementos simbólicos como la fraternidad islámica, el sufrimiento de los musulmanes o la gloria del martirio.

Esta persona, según los informes policiales, manifestaba en sus comunicaciones una admiración casi romántica por el califato, interpretando su viaje a zona de conflicto sirio-iraquí como un acto de purificación espiritual y redención, tal y como se evidenció en la vista judicial, pues el detenido:

Había intentado viajar a Siria a través de Turquía, para lo que adquirió un billete de ida para el 10 de enero del 2015 y reservó un hotel en Estambul para los días 10 y 12, sin embargo no pudo viajar al no permitir la compañía aérea el embarque, al exigirse por las autoridades turcas como medida preventiva para entrar en ese país el estar en posesión por un billete de vuelta. (EFE, 2015)

Hechos que permiten inferir, que tras su jura de fidelidad a Daesh, su intención no era otra que el martirio por la causa de Allah. Esta dimensión mística del radicalismo dificulta su detección mediante mecanismos tradicionales de prevención. No había conspiración organizada, ni células físicas, ni planificación táctica: solo una intención radical, silenciosa y en evolución digital.

Casos como el de Benkaddour en los que las FCSE eran pioneros, y el Servicio de Información de la Guardia Civil de Murcia junto con la Unidad Central Especial nº 2 de la Jefatura de Información de la Guardia Civil, prácticamente levantaban jurisprudencia a través de esta detención, revelan que la prevención ya no puede

depender exclusivamente de la vigilancia física o la inteligencia obtenida a través del entorno u confidentes al uso, sino que debe incorporar herramientas de monitoreo y actuación encubierta en espacios digitales, donde se forjan estos nuevos perfiles.

Fruto de las incipientes detenciones de estos nuevos individuos de la yihad digital junto a la avalancha de *foreign fighters* residentes en España que emigraban a combatir en las filas de la organización terrorista Daesh, quedó en evidencia la necesidad urgente de figuras legales que permitieran la infiltración en redes sociales, foros y canales encriptados, no para castigar a posteriori, sino para anticiparse a la consumación del delito. En ese sentido, la figura del Agente Encubierto Informático se configuró como la única herramienta capaz de penetrar ese tipo de entramados sin comprometer garantías constitucionales, especialmente en fases embrionarias de captación.

11.2. EL AGENTE ENCUBIERTO INFORMÁTICO

La consolidación jurídica del Agente Encubierto Informático en el proceso penal español se produjo a través de la Ley Orgánica 13/2015, de 5 de octubre, de modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica, que reformó la Ley de Enjuiciamiento Criminal con el propósito de reforzar las garantías procesales y dotar al sistema de herramientas eficaces frente a los desafíos tecnológicos emergentes. Esta reforma no fue una mera actualización técnica, sino que supuso un auténtico punto de inflexión en la investigación de fenómenos tan complejos como el terrorismo y la criminalidad organizada, al permitir una integración normativa explícita de nuevas metodologías adaptadas al nuevo paradigma digital,

Dicha ley supuso un hito en la persecución penal de delitos cometidos en entornos digitales donde la huella del autor se torna binaria, efímera y encriptada; al introducir explícitamente en el artículo 282 bis las facultades del agente encubierto para actuar en canales de comunicación cerrados bajo identidad supuesta. Así lo establece el tenor literal del Artículo 282 bis.6 LECrim:

El juez de instrucción podrá autorizar a funcionarios de la Policía Judicial para actuar bajo identidad supuesta en comunicaciones mantenidas en canales cerrados de comunicación con el fin de esclarecer alguno de los delitos a los que se refiere el apartado 4 de este artículo o cualquier delito de los previstos en el artículo 588 ter a.

El agente encubierto informático, con autorización específica para ello, podrá intercambiar o enviar por sí mismo archivos ilícitos por razón de su contenido y analizar los resultados de los algoritmos aplicados para la identificación de dichos archivos ilícitos. (BOE, 2015)

Este precepto no constituye una innovación absoluta, sino la positivización de una práctica que por analogía venía siendo admitida por la doctrina jurisprudencial bajo el principio de necesidad y proporcionalidad. Ya que, la figura del Agente Encubierto Informático no es un tipo distinto al del Agente Encubierto “clásico”, sino que es una modalidad operativa del mismo. Así lo expresó el Magistrado-Juez de la Audiencia Nacional José De la Mata, quien señala que: “a todos los efectos, el Agente Encubierto Informático es un Agente Encubierto. Y, por tanto, no es algo distinto, por lo que se le aplica el estatuto y el régimen propio del Agente Encubierto”, si bien con las particularidades propias de su actuación en el ámbito virtual (De la Mata, 2017).

Ahora bien, por primera vez se desarrolla un artículo que permite el envío de archivos ilícitos como parte de la labor de infiltración, siempre que se cumplan dos condiciones inexcusables: que exista una autorización judicial específica y que el archivo tenga como finalidad exclusiva el esclarecimiento de delitos graves y concretos previamente investigados. Esta habilitación se justifica porque en el mundo digital la simple observación pasiva no permite desvelar intenciones

delictivas ni acceder a contenidos ocultos tras mecanismos de confianza que requieren interacción activa.

No obstante, esta facultad no convierte al agente en un provocador. Muy al contrario, el artículo 282 bis.5 LECrim traza una línea clara al afirmar que el agente encubierto: “estará exento de responsabilidad criminal por aquellas actuaciones que sean consecuencia necesaria del desarrollo de la investigación, siempre que guarden la debida proporcionalidad con la finalidad de la misma y no constituyan una provocación al delito” (BOE, 1999).

La frontera entre infiltración legítima y provocación ilegítima ha sido perfilada por la jurisprudencia del Tribunal Supremo, que advierte, por ejemplo, en la STS 575/2013, que “el delito provocado se configura cuando el agente induce al investigado a delinquir, generando una conducta que no se habría producido espontáneamente”. Por tanto, el AEI solo podrá actuar para observar, documentar o participar de forma pasiva en dinámicas ya existentes, pero nunca para crear la situación delictiva que se desea investigar.

En coherencia con ello, la LECrim contempla mecanismos de control jurisdiccional reforzado para evitar abusos. Así, el artículo 282 bis.3 prevé que “cuando las actuaciones de investigación puedan afectar a los derechos fundamentales, el agente encubierto deberá solicitar del órgano judicial competente las autorizaciones que, al respecto, establezca la Constitución y la Ley, así como cumplir las demás previsiones legales aplicables” (BOE, 1999).

Esto se materializa, por ejemplo, en el caso del artículo 282 bis.7, que introduce la posibilidad de grabar conversaciones o captar imágenes en el interior de domicilios durante encuentros programados con el investigado, siempre que haya una autorización judicial expresa. Tal medida, por su carga intrusiva, solo puede adoptarse si se respetan los principios de necesidad, idoneidad y proporcionalidad, en línea con la jurisprudencia constitucional (STS 1546/2016).

Esta disposición no solo amplía el alcance funcional del AEI, sino que sitúa al juez de instrucción como garante último del equilibrio entre eficacia investigadora e integridad de las libertades públicas. Como establece el Tribunal Constitucional en su STC 114/1984, “las limitaciones a derechos fundamentales solo pueden justificarse cuando son necesarias, proporcionadas y están previstas por una norma

con rango de ley”. Por ello, el control judicial previo, lejos de ser un trámite formal, debe apoyarse en una valoración concreta de los hechos, los riesgos y la imposibilidad de obtener la información por medios menos invasivos. Así lo exige también el artículo 386 del Anteproyecto de LECrim de 2020, que detalla los requisitos para autorizar escuchas privadas cuando participa un AEI, como son la existencia de indicios objetivos de un delito grave, en la que tenga cabida investigativa un Agente Encubierto; que se prevean conversaciones que puedan ser relevantes para la causa; y la ausencia de medidas alternativas menos gravosas (Consejo de ministros, 2020).

En paralelo, el artículo 410 del mismo texto proyecta una regulación del consentimiento domiciliario que incluye la posibilidad de entrada del AEI en un domicilio bajo identidad falsa, “si ha sido autorizado por el juez de garantías”.

Este nuevo cuerpo normativo también actualiza la estructura de protección jurídica del propio agente. El artículo 504 del Anteproyecto reconoce expresamente que la identidad falsa será asignada por el Ministerio del Interior, con plena validez para actuar en el tráfico jurídico y social, y que dicha identidad se conservará en pieza separada y secreta a disposición exclusiva del juez competente. De esta manera, se protege no solo la integridad del agente, sino la eficacia operativa de su labor y la cadena de custodia probatoria (Consejo de ministros, 2020).

Asimismo, el artículo 507 del Anteproyecto autoriza que el agente encubierto pueda declarar en juicio bajo su identidad ficticia cuando así se justifique por razones de seguridad, siguiendo criterios establecidos por el Tribunal Europeo Derechos Humanos (TEDH) en casos como Van Mechelen vs. Netherlands (1997), siempre que la defensa pueda contradecir de forma efectiva su testimonio.

Por último, toda prueba obtenida por el AEI debe ser sometida a un control estricto en la cadena de custodia digital, conforme a los artículos 588 sexies y siguientes de la LECrim. Esta trazabilidad es especialmente crítica en contextos donde el material probatorio se basa en archivos digitales (mensajes, vídeos, claves, IP), como se señaló en la sentencia de la Audiencia Provincial de Islas Baleares, que valoró como válida una prueba por AEI al documentarse forensemente toda la obtención, conservación y trazabilidad de los contenidos (SAP IB 854/2021)

En definitiva, el agente encubierto informático no es una figura ajena o nueva, sino una evolución operativa del agente encubierto “clásico” en entornos virtuales.

Su regulación exige un equilibrio delicado entre eficacia investigadora y respeto a los derechos fundamentales, un control judicial permanente y una rigurosa trazabilidad de la prueba. Pero bien ejecutada, esta herramienta se erige como una de las más potentes del Derecho moderno frente a las nuevas formas de criminalidad, ausentes de fronteras físicas, ni estructuras jerárquicas visibles, sino redes fluidas, anónimas y altamente capacitadas.

A la luz de lo anterior, y para comprender con mayor precisión el alcance jurídico-operativo del Agente Encubierto Informático, conviene sistematizar los requisitos que rigen su actuación. Estos se estructuran sobre la base del marco normativo general previsto para el agente encubierto clásico, al que se suman, tras la reforma introducida por la Ley Orgánica 13/2015 y las previsiones del Anteproyecto de LECrim de 2020, una serie de condiciones específicas orientadas a su despliegue en el ciberespacio:

1. **Sujetos legitimados para actuar como AEI:** Al igual que el agente encubierto clásico, solo podrán actuar bajo identidad supuesta quienes sean funcionarios de las Fuerzas y Cuerpos de Seguridad que ejerzan funciones de Policía Judicial, excluyendo expresamente a los particulares, confidentes o arrepentidos (art. 282 bis.1 LECrim; art. 501 Anteproyecto LECrim). Deben ser “especialmente seleccionados” en virtud de su preparación técnica, experiencia previa y capacitación operativa en entornos digitales.
2. **Autorización motivada:** La intervención del AEI requiere autorización expresa y motivada del juez de instrucción. En casos de urgencia, el Ministerio Fiscal puede autorizar de forma provisional, dando cuenta inmediata al juez. La autorización debe recoger tanto la identidad real como la ficticia, en documento reservado y custodiado por el órgano judicial (art. 282 bis.1 LECrim; arts. 502 y 503 Anteproyecto LECrim).
3. **Duración de la medida:** El uso de identidad encubierta tendrá una duración inicial de seis meses, prorrogables por periodos de igual duración previa nueva resolución judicial motivada. Así lo dispone tanto el artículo 282 bis.1 LECrim como el artículo 503.1.f del Anteproyecto.

4. **Ámbito delictivo objetivo:** La actuación del AEI se restringe a la investigación de delitos graves relacionados con el crimen organizado, tipificados en el artículo 282 bis.4 LECrim: terrorismo, trata de seres humanos, pornografía infantil, corrupción, tráfico de armas o drogas, entre otros. La reforma de 2015 amplió expresamente este catálogo para incluir delitos cometidos mediante las Tecnologías de la Información y las Comunicaciones (art. 588 ter a LECrim) y aquellos que exijan infiltración en canales cerrados de comunicación.
5. **Principio de idoneidad:** Ya que lo que se investigan son conductas realizadas por ciberdelincuentes en Internet. Además de las facultades comunes al agente encubierto clásico (participación en el tráfico jurídico, interacción con sospechosos, obtención de pruebas...), el AEI puede realizar acciones propias del ciberespacio:
 - Acceder a canales cerrados de comunicación bajo identidad falsa.
 - Intercambiar o remitir archivos ilícitos por razón de su contenido (previa autorización judicial).
 - Analizar resultados de algoritmos de detección de contenido delictivo.
 - Realizar captación de imágenes y sonido en entornos cerrados, incluidos domicilios (art. 282 bis.6 y 7 LECrim; arts. 386 y 413 Anteproyecto LECrim).
6. **Principio de proporcionalidad y protección reforzada de derechos fundamentales:** Toda actuación del AEI deberá ser menos lesiva que el delito investigado. Así como cualquier vulneración que implique afectación de derechos fundamentales como la intimidad, el secreto de las comunicaciones (art. 18.3 CE) o la inviolabilidad del domicilio (art. 18.2 CE) requiere autorización judicial específica y motivada. Esto se regula en el artículo 282 bis.3 LECrim y se desarrolla en el artículo 505 del Anteproyecto, que distingue entre la mera infiltración digital (con menor afectación) y otras medidas más intrusivas (escucha, entrada en domicilio).
7. **Interdicción de la provocación delictiva:** El AEI tiene terminantemente prohibido instigar, inducir o promover conductas delictivas que no hayan

surgido de forma autónoma por el investigado. Solo podrá actuar como observador o receptor pasivo, y en ningún caso fabricar pruebas ni inducir al error (art. 282 bis.5 LECrim; art. 506 Anteproyecto). La jurisprudencia es clara: el delito provocado invalida la prueba y contamina todo el procedimiento (STS 575/2013).

8. **Exención de responsabilidad penal condicionada:** El AEI queda exento de responsabilidad penal únicamente por aquellas conductas que sean necesarias, proporcionadas y directamente relacionadas con el objeto de la investigación. Esta excusa absolutoria se recoge en el artículo 282 bis.5 y se matiza en el art. 506.2 del Anteproyecto: no debe afectarse un bien jurídico superior ni excederse en la medida adoptada.
9. **Identidad supuesta o simulada:** La identidad ficticia debe ser otorgada por el Ministerio del Interior (art. 282 bis.1 y art. 504 Anteproyecto). Incluye nombre, documentación, perfiles virtuales y cobertura digital en redes, foros o canales cifrados. Se puede usar incluso en sede judicial, sin revelar la identidad real, siempre que lo autorice el juez (art. 282 bis.2 LECrim; art. 507 Anteproyecto).
10. **Obligación de preservar la cadena de custodia digital:** Toda prueba digital obtenida por el AEI debe ser recogida conforme a protocolos forenses homologados, con sellado hash, logs, evidencias de volcado y sin alteración de metadatos. La cadena de custodia debe quedar garantizada desde la obtención hasta la exhibición en juicio (art. 588 sexies LECrim; SAP Illes Balears 854/2021; STS 489/2020).
11. **Testimonio protegido y validez probatoria:** El AEI puede declarar en juicio manteniendo su identidad falsa si así lo autoriza el juez, garantizando el principio de contradicción (art. 282 bis.2 LECrim; STS 1140/2010). La prueba debe ser corroborada por otros elementos objetivos, conforme al principio de valoración racional.

12. **Principios de necesidad y excepcionalidad:** El uso del AEI debe ser la última ratio investigativa. Solo puede emplearse si no existen otros medios menos invasivos para descubrir la verdad y debe mantenerse control judicial durante toda la operación (art. 386 Anteproyecto LECrim). El principio de subsidiariedad es fundamental para justificar la legitimidad de la medida.

11.3. REQUISITOS POLICIALES Y OPERATIVOS DEL AGENTE ENCUBIERTO INFORMÁTICO

La figura del Agente Encubierto Informático, como prolongación operativa de su homólogo tradicional, no puede concebirse únicamente desde la óptica de su habilitación legal y judicial conforme al artículo 282 bis de la Ley de Enjuiciamiento Criminal. Su eficacia real descansa, además, en un conjunto de condiciones personales, competencias técnicas y capacidades operativas que exceden con mucho el marco jurídico. En contextos tan sensibles como el del terrorismo yihadista, un solo desliz en la actuación del AEI no compromete únicamente la validez de una prueba o la viabilidad de una operación: puede poner en peligro su propia integridad física y la de su familia.

En este entorno altamente volátil, donde el adversario actúa desde el anonimato, se camufla con identidades múltiples y despliega técnicas de contrainteligencia en tiempo real, no basta con el respaldo normativo. Es imprescindible una preparación especializada que abarque desde el conocimiento de los entornos virtuales clandestinos hasta la comprensión psicológica del perfil yihadista. Solo así, el AEI podrá transitar con solvencia los márgenes más oscuros del ciberespacio, donde la ley se entrelaza con la amenaza, y la seguridad personal se convierte en una línea tan frágil como invisible.

A continuación, se detallan los principales requisitos y fases operativas que debe asumir el funcionario designado como AEI:

1. **Ciberpatrullaje digital:** Antes de que el Agente Encubierto Informático entre en acción, resulta imprescindible considerar el valor operativo del ciberpatrullaje digital, entendido como una labor de observación discreta,

sistemática y no intrusiva de contenidos y actividades accesibles en la red. Esta práctica, enmarcada dentro de las funciones ordinarias de prevención y detección de delitos atribuidas a las Fuerzas y Cuerpos de Seguridad, permite a los investigadores detectar fenómenos incipientes de radicalización, delitos en curso o patrones de riesgo, sin que ello implique una afectación a derechos fundamentales.

En efecto, mientras no se supere el umbral de acceso a información privada o restringida, la mera observación de foros públicos, redes sociales abiertas, blogs o contenidos visibles en motores de búsqueda no requiere autorización judicial, ya que se considera una actividad legítima al tratarse de espacios abiertos a terceros.

Esta práctica ha sido avalada por la jurisprudencia española. En la Sentencia de la Audiencia Nacional 30/2020, de 14 de febrero, se validó la actuación de la Guardia Civil que, mediante técnicas OSINT⁹ y sin injerencia directa, logró detectar a un usuario que difundía contenido yihadista en canales abiertos. El tribunal entendió que no existió vulneración del derecho a la intimidad, dado que toda la información recabada se encontraba publicada voluntariamente por el investigado en espacios públicos de acceso libre.

Asimismo, el Tribunal Supremo, en su STS 173/2021, de 17 de marzo, ratificó que el análisis de contenidos publicados en Twitter, incluso cuando el perfil no emplea nombre real, no exige cobertura legal reforzada, al tratarse de información libremente accesible para cualquier usuario conectado a la red.

Este tipo de actuaciones, denominadas también “vigilancia pasiva” o “navegación policial”, forman parte del arsenal metodológico de la ciberinteligencia policial y constituyen el paso previo a la activación de medidas más intrusivas, como el uso de identidades encubiertas o la interceptación de comunicaciones.

Por tanto, el ciberpatrullaje permite recabar información clave para:

- Identificar comunidades o perfiles sospechosos.
- Observar interacciones o narrativas preocupantes.

⁹ Obtención de información en fuentes abiertas, que son públicas o accesibles por cualquier usuario.

- Cartografiar redes o relaciones digitales.
- Obtener indicios razonables que justifiquen la solicitud de una medida de AEI o intervención tecnológica.

2. Valoración de la necesidad y proporcionalidad de la medida: La activación de un Agente Encubierto Informático no puede responder a una decisión precipitada o genérica. Su uso exige una ponderación rigurosa de necesidad, idoneidad y proporcionalidad, conforme a los principios rectores de toda injerencia en derechos fundamentales. La infiltración digital, en particular, requiere un despliegue complejo de recursos técnicos, humanos y logísticos, por lo que sólo debe autorizarse cuando no existan otros medios menos invasivos que permitan alcanzar los mismos fines investigativos.

En fases preliminares de la investigación, cuando el objetivo esté limitado a observar foros abiertos, publicaciones en redes sociales o canales públicos, puede bastar con el uso de técnicas OSINT, sin necesidad de una identidad encubierta formalmente constituida. Sin embargo, en cuanto se pretende acceder a grupos cifrados, comunidades cerradas o conversaciones privadas, la operativa exige cobertura legal reforzada bajo la forma de AEI, debidamente autorizada por el juez competente.

3. Selección y perfil operativo del agente: No todo miembro de las Fuerzas y Cuerpos de Seguridad está capacitado para asumir las funciones de Agente Encubierto Informático. Se requiere una selección escrupulosa en base a criterios de idoneidad, solvencia emocional, experiencia operativa y especialización técnica. El agente designado debe acreditar dominio en materias como:

- Ciberinteligencia y detección de patrones delictivos en la red.
- Análisis de fuentes abiertas (OSINT) y de redes sociales (SOCMINT).
- Técnicas de infiltración en entornos digitales y creación de las coberturas y avatares digitales.

- Conocimiento de metodología OPSEC¹⁰, que garantice la seguridad de sus acciones, a través del empleo de redes privadas virtuales (VPN) y navegación por la dark web.
- Psicología del comportamiento criminal y radicalización online.
- De forma especial, debe ser entrenado en Virtual HUMINT, esto es, la capacidad de interactuar con personas reales a través de identidades simuladas, creando relaciones de confianza digital sin despertar sospechas. Esta habilidad exige empatía estratégica, adaptación lingüística y narrativa, y control emocional en escenarios de alto riesgo.

4. Infraestructura técnica y dispositivos asociados: La experiencia demuestra que las comunicaciones con los investigados rara vez se limitan a una sola plataforma. Es frecuente que, tras una toma de contacto inicial en una red abierta, la conversación migre a aplicaciones más seguras como Telegram, Signal, Threema o foros alojados en la dark web. Por ello, el AEI debe disponer de varios dispositivos independientes (ordenador portátil y teléfono móvil principalmente), cada uno con sistemas de cifrado, configuraciones de seguridad y herramientas de monitorización adaptadas al entorno.

Además, estos dispositivos deben ser controlados y auditados por la unidad técnica correspondiente, garantizando la cadena de custodia digital y la integridad de las evidencias obtenidas. El uso de herramientas forenses, firmas digitales, registros hash y protocolos de volcado seguro son imprescindibles.

5. Acta de constitución y resolución judicial motivada: Una vez autorizada judicialmente la medida, el agente deberá constituirse formalmente como AEI ante el Juzgado de Instrucción competente. En ese acto, se levantará un acta donde consten su identidad real, la identidad simulada, los perfiles

¹⁰ En el argot militar, Operational Security (OPSEC), hace referencia al conjunto de medidas tendentes a evitar que posibles adversarios descubran información clasificada o necesaria para mantener la seguridad de los Agentes y confidencialidad de la misión.

creados, los dispositivos que empleará y el ámbito temporal y funcional de su autorización. Esta resolución será reservada y se conservará en pieza separada, conforme al artículo 282 bis.1 de la LECrim.

6. **Paciencia en la interacción con los objetivos y gestión del riesgo operativo:** El momento crítico de toda operación encubierta llega con la interacción directa con el investigado. En este punto, el Agente debe mantener el equilibrio entre obtener información relevante y no comprometer su cobertura. Cada mensaje, cada archivo enviado, cada comentario puede ser utilizado por el investigado para verificar la autenticidad del perfil. Además, el AEI debe estar preparado para escenarios de "prueba de lealtad" o "retos de confianza" (como compartir contenido sensible o participar en foros extremistas), que pondrán a prueba su credibilidad sin traspasar los límites legales.
7. **Conocimiento de la amenaza y concordancia lingüística:** El perfil o avatar virtual que emplee el AEI en su aproximación a los objetivos debe ser coherente con el entorno social, idiomático y cultural del grupo investigado. No es lo mismo infiltrarse en un foro neonazi en español, que en una comunidad yihadista francófona. El dominio del lenguaje, su jerga, la religión, la historia, hasta los horarios de conexión para interactuar con los objetivos deben estar alineados. Por todo ello, la construcción de la narrativa debe ser coherente, verificada y flexible.

XII – EL AGENTE ENCUBIERTO INFORMÁTICO COMO HERRAMIENTA DE PREVENCIÓN DEL TERRORISMO YIHADISTA

XII - EL AGENTE ENCUBIERTO INFORMÁTICO COMO HERRAMIENTA DE PREVENCIÓN DEL TERRORISMO YIHADISTA

12.1. DINÁMICAS DE RADICALIZACIÓN ONLINE EN ESPAÑA ANTES DE LA L.O 13/2015

Durante la primera década del siglo XXI, la amenaza yihadista en España estuvo marcada por estructuras operativas tradicionales, células logísticas vinculadas a Al Qaeda y actividades de financiación. Sin embargo, con la irrupción del conflicto sirio y la proclamación del Califato del Daesh en 2014, emergió un nuevo tipo de activismo radical: jóvenes conectados desde sus domicilios, alfabetizados tecnológicamente, que utilizaban las redes sociales, los foros islámicos y las plataformas cifradas para difundir odio, reclutar adeptos y adoctrinar en la violencia.

Uno de los casos paradigmáticos que reflejan este giro operativo fue el de Faiçal Errai, detenido en Valencia en 2012 y conocido como el bibliotecario de Al Qaeda. A través de su actividad digital, Errai recopilaba, traducía y distribuía materiales de adoctrinamiento, incluyendo manuales operativos, sermones radicales y publicaciones de corte salafista-yihadista. Su perfil encarnaba el nuevo modelo de predicador virtual, más peligroso si cabe por su invisibilidad y por la amplitud de su red de contactos (El País, 2016).

La Sentencia de la Audiencia Nacional SAN 3380/2013 expone que Faiçal Errai utilizaba múltiples cuentas y metodologías de anonimización digital, para la creación de foros privados destinados a la formación y captación de militantes que ingresaran en las filas de Al-Qaeda, llegando a admitir en su juicio que:

Ansar Al Mujahideen era una estructura yihadista, que estaba integrada por una serie de personas, que desarrollaba actividades de propaganda, formación religiosa y política y captación de militantes para que actuaran como muyahidines en los conflictos abiertos en Chechenia,

Afganistán o Somalia. Reconoció que participaba en la red y en el foro. Para ello, había adquirido hasta treinta y cinco dominios de Internet. Uno de éstos, *www.ansaralyihad.net*, se lo cedió a Mr_ 56, administrador del foro yihadista, que vivía en Arabia Saudita, para que alojara el foro. En los foros llegaban a participar más 2000 personas. Después había salas más reservadas, controladas por el programa *paltalk*, y canales para comunicarse de manera privada. Esos eran los mecanismos de selección y captación.

Junto a los foros públicos en las que intervienen todo tipo de personas, situadas incluso en las zonas de conflicto, están las salas de acceso restringido, salas *paltalk*, controladas por los supervisores, quienes permiten y niegan el acceso. Y, en última instancia existe la posibilidad de establecer comunicaciones particulares de carácter secreto. Refirió que jóvenes como él quedan atrapados en los foros a través de técnicas de control mental, que utilizan para manejar al individuo como si fuera una marioneta. Para convertir a alguien ya motivado en un mártir dispuesto a inmolarse, manifestó el acusado, se requiere un largo proceso de radicalización y formación religiosa. En las salas *paltalk* había cientos de personas que querían irse a Siria y a otros lugares de conflicto. Los dirigentes de la sala eran los que controlaban y seleccionaban a la gente,

determinaban quién era apto para actuar como muyahidines, y tras ello a algunos se les permitía el acceso a campos de entrenamiento.

Se servía de programas de encriptación proxy y utilizaba varios nicks [...] Cuando se ganó la confianza de los administradores de la red le encargaron administrar y supervisar algún foro o sala; lo que era un orgullo. Mencionó a varias personas que habían partido como muyahidines hacia Waziristán (región de Pakistán, limítrofe con Afganistán), etc. (SAN 3380/2013)

Su condena por enaltecimiento del terrorismo y tenencia de material para la radicalización evidenció la urgente necesidad de legislar mecanismos de investigación adaptados al entorno digital, así como la adecuación del Código Penal. A pesar del éxito operativo, los investigadores carecían de herramientas para interactuar encubiertamente con su red de contactos o infiltrarse en las plataformas donde se gestaba el odio. Este vacío normativo reveló que el sistema jurídico español necesitaba dar el salto desde la observación pasiva hacia la infiltración activa en entornos digitales.

Si Errai representó el adoctrinamiento, Mustafá Maya Amaya encarnó la captación. Convertido al islam en los años 90, este ciudadano español de etnia gitana y origen navarro, afincado en Melilla, se convirtió en el principal reclutador de combatientes para Siria e Iraq desde territorio español, con más de 50 envíos confirmados a zonas de conflicto entre 2012 y 2014 (El Mundo, 2015). En las redes sociales, se le conocía como Abu Salma, y su perfil no levantaba sospechas, pues era un hombre mayor, con movilidad reducida y sin antecedentes penales graves.

La investigación conjunta de la Policía Nacional y el Centro Nacional de Inteligencia, bautizada como Operación Azteca, reveló que Mustafá dirigía desde su casa una compleja red transnacional de reclutamiento online. Mediante Facebook, YouTube y Skype adoctrinaba a jóvenes de Ceuta, Melilla, Bélgica, Francia, Siria y Túnez, facilitándoles contactos, instrucciones, financiación para el

viaje y hasta juramentos de lealtad al Daesh. La Audiencia Nacional lo consideró un “verdadero nodo transnacional de captación” (El País, 2014).

Su caso puso en evidencia una laguna operativa estructural: no existía todavía una cobertura legal eficaz para infiltrar sus redes virtuales en tiempo real. De haberse contado con agentes encubiertos digitales debidamente autorizados, muchas de las captaciones podrían haberse interrumpido antes de que los jóvenes viajaran al teatro de operaciones. Su detención, junto con otros miembros de la red, fue un hito, pero también una lección institucional: el enemigo ya no está necesariamente en la mezquita o la calle, sino en el algoritmo, el perfil social y el chat encriptado.

Junto a los casos emblemáticos de Faïçal Errai y Mustafá Maya Amaya, surgió en torno al año 2014 una oleada de jóvenes de origen magrebí, muchos de ellos nacidos, residentes o con fuertes vínculos en España que, captados a través de canales digitales, abandonaron sus hogares para unirse a las filas del Estado Islámico en Siria e Iraq. Su perfil era alarmantemente homogéneo: varones entre 19 y 30 años, sin apenas formación superior, socializados en barrios periféricos con escasa integración, pocas opciones de forjarse un futuro lejos de la delincuencia y expuestos a narrativas de exclusión identitaria.

Uno de los más conocidos fue Mohammed Ghobrit, un joven proveniente de Tetuán (Marruecos), ciudad a pocos kilómetros con la frontera de Ceuta, que residía en Tarragona y viajó a Siria con apenas 20 años, quién acabó enrolado en el en un batallón de Daesh junto a su hermano Marouan Ghobrit, pocos años mayor que él. Las autoridades españolas confirmaron su fallecimiento en 2016, tras varios meses difundiendo imágenes junto a otros yihadistas de su ciudad, armas y vida “heroica” en redes sociales, destinadas a seducir a nuevos reclutas (La Verdad, 2016).

Otro caso conmovedor fue el de Nabil Benkkadour, detenido en 2015 en San Pedro del Pinatar (Murcia), a punto de viajar a zona de conflicto. Su caso fue paradigmático pues mantenía actividad intensa en redes, juró fidelidad al Daesh en vídeos alojados en plataformas virtuales abiertas, y fue identificado por Guardia Civil y detenido de forma preventiva, gracias a labores de ciberpatrullaje digital (El Mundo, 2015).

Inmersos en esta corriente yihadista, figuran otros nombres clave como, Mohamed Tarik, Abdallah Guitone, quienes no dudaban en afirmar a través de sus redes sociales que atacarían nuestro país: “atacaremos pronto, primero en España, después en Marruecos y Roma”, “os atacaremos en vuestras iglesias, en vuestros ayuntamientos y comisarías”, (Gil, 2014). Junto a otros como Imad Jibar, conocido por sus vínculos con células de reclutamiento catalanas; “Kokito Castillejos”, apodo de Mohamed Hamdouch, un joven de origen ceutí que alcanzó notoriedad por aparecer en vídeos del Daesh posando con cabezas decapitadas y promoviendo ataques en España y el resto de Europa; o Redouane el Haddouti, responsable de tareas logísticas en Siria y vinculado a redes de captación en Melilla y Bélgica (Gil, 2014).

Todos ellos formaron una generación de jóvenes yihadistas, que se encontraba atrapada entre dos culturas, discursos de marginación, y finalmente seducida por una promesa de identidad absoluta en el Califato de Daesh, junto a una causa trascendental y “honor global” mediante el martirio en el camino de Allah. Ninguno de estos casos habría podido prevenirse eficazmente sin herramientas específicas de detección temprana en el ciberespacio que únicamente podían realizarse a través de misiones de ciberpatrullaje digital. Por todo ello, la necesidad de incorporar a nuestro ordenamiento jurídico una figura investigativa como el Agente Encubierto Informático se hizo entonces imprescindible, pues la simple observación de foros abiertos y redes sociales no bastaba para penetrar los entornos verdaderamente operativos: chats cerrados, canales cifrados, plataformas anonimizadas y redes distribuidas transnacionalmente.

A continuación, se expone un análisis riguroso de las operaciones policiales más destacadas de los últimos años, con el estudio detallado de las sentencias judiciales en las que la actuación del AEI ha sido determinante para la detección, infiltración y desarticulación de redes yihadistas en España.

12.2. JURISPRUDENCIA Y EFICACIA OPERATIVA DEL AGENTE ENCUBIERTO INFORMÁTICO EN LA LUCHA CONTRA EL TERRORISMO YIHADISTA

12.2.1. Diligencias Previas 27/2016 del Juzgado Central de Instrucción número 2 de la Audiencia Nacional, SAN 5286/2019, SAN 2203/2020 y STS 3448/2020: Operación Trankilo.

- **Contextualización del caso:**

El 5 de diciembre de 2017, varios medios nacionales e internacionales difundieron la detención de Mustapha El Filali en la localidad de Parla (Madrid), en el marco de una Operación policial en la que días antes habían detenido a los hermanos Mohsin Harrak y Anouar Harrak en Figueres, bajo los siguientes titulares:

“El acusado de yihadismo planeó atropellos con coche bomba en el centro de Madrid”
(La Razón, 2019)

“Juzgado un yihadista que planeó un atropello masivo en la Puerta del Sol en Navidad” (El Mundo, 2019)

“La Audiencia Nacional juzga a tres yihadistas que contaron sus planes de atentar en España a un agente encubierto” (Servimedia, 2019)

- **Análisis de las sentencias:**

Derivado de la mencionada “Operación Trankilo”, realizada por la Policía Nacional en el marco de las Diligencias Previas Procedimiento Abreviado 27/2006 dimanantes del Juzgado Central de Instrucción número 2 de la Audiencia Nacional en Madrid, SAN 5286/2019, SAN 2203/2020 y STS 3448/2020, se constató la intervención de al menos dos Agentes Encubiertos Informáticos bajo los alias “Amira Chafchaf” y “Ahmed Bouali”, quienes entraron en contacto directo con los detenidos.

Mustapha El Filali, se presentó en redes sociales como usuario fervientemente vinculado al ideario de Daesh. Según consta en medios de prensa y en el Auto judicial uno de los AEI, simuló ser una joven granadina con quien el

investigado compartía propaganda y mantenía conversaciones con alto contenido yihadista.

En este caso, el AEI a través de las conversaciones mantenidas con el acusado fue fundamental para obtener evidencia directa del propósito del acusado de cometer un atentado en Madrid durante las fiestas navideñas, a través de una metodología similar al perpetrado en agosto de dicho año en las Ramblas de Barcelona, el atropello. Y para ello, estaba intentando conformar en España una célula operativa de yihadistas de idéntica adscripción dispuestos al martirio en nombre de Daesh.

En palabras del propio investigado a través de reiteradas confidencias con los AEI:

Cerca de la plaza del Sol, pero en navidades. Más gente es caos, mucha mucha gente. Es Madrid y hay más calles llenas. Hay cuatro calles peatonales en la misma zona y están juntas. [...] calles peatonales masivamente concurridas ubicadas en el centro de Madrid, mediante un vehículo de grandes dimensiones en las próximas navidades para causar el mayor número de víctimas posibles, y reivindicado en nombre de Daesh con el martirio. (DP 17/2016)

Desde una perspectiva jurídica y operativa, la labor de los AEI fue determinante. A través del engaño controlado y autorizado judicialmente, permitió recopilar pruebas anticipadas del propósito criminal, evitando que el investigado alcanzara una fase de ejecución. Así, las conversaciones sostenidas con los agentes encubiertos virtuales no solo sirvieron para esclarecer la fase de planificación, sino también para probar la existencia de redes de colaboración.

Hecho especialmente relevante es que en dicha sentencia, se expone como el acusado trató de “calibrar la disposición al martirio” de la Agente bajo el alias “Amira Chafchaf”. Además, contactó con otro agente encubierto bajo el alias “Ahmed Bouali”, consolidando un patrón de interacción con miembros

encubiertos que demuestra el uso operativo de estos en diferentes frentes (DP 17/2016 y STS 3448/2020)

De la información recabada en el auto judicial se deduce que Mustapha El Filali no solo se encontraba en una fase avanzada de planificación de atentado, sino que también realizaba labores de captación y adoctrinamiento. Según el auto:

Se ha constatado que Mustapha El Filali formaría parte de la organización terrorista Daesh, para la que ha venido realizando actividades como la planificación de un atentado en Madrid, la captación y adoctrinamiento a través de redes sociales, y la divulgación de propaganda oficial de la organización terrorista.

- **Valoración jurídica de la medida:**

El uso de los agentes encubiertos fue autorizado conforme al artículo 282 bis de la Ley de Enjuiciamiento Criminal, el cual permite, mediante autorización judicial, la interacción controlada en entornos digitales con el fin de prevenir delitos graves. Se respetaron los principios de proporcionalidad y subsidiariedad, al tratarse de un delito extremadamente grave como es el terrorismo yihadista con riesgo de atentado masivo.

La prueba derivada de la intervención del AEI es plenamente válida, al haberse obtenido mediante autorización judicial y no haber mediado provocación al delito, sino revelación delictiva. Las conversaciones intervenidas y reproducidas en los autos muestran una iniciativa activa y previa del acusado hacia la comisión del delito.

- **Impacto preventivo y simbólico de la operación:**

Desde el punto de vista operativo y social, la operación tuvo un alto impacto preventivo. Se logró dismantelar una célula yihadista que pretendía atacar en fechas señaladas en un lugar emblemático y altamente concurrido en la Puerta del Sol (Madrid), lo cual habría causado una catástrofe.

El valor simbólico de frustrar un atentado en fechas navideñas, en pleno centro de la capital, tuvo un efecto disuasorio y reafirmó la eficacia de las técnicas

de infiltración digital como medida de preventiva de contrainteligencia contra el terrorismo de etiología yihadista.

- **Conclusión:**

Este caso pone de manifiesto el papel fundamental que desempeña el Agente Encubierto Informático en la prevención del terrorismo yihadista en el ámbito digital. Su actuación, cuando es jurídicamente autorizada, técnica y éticamente calibrada, permite descubrir hechos antes de que resulten irreparables. En el caso de El Filali, su interacción con agentes virtuales permitió detener a una célula con intenciones homicidas, sin vulnerar derechos fundamentales.

12.2.2. Sumario 8/2016, SAN 3462/2018, STS 750/2019 y ATS 5261/2019: Operación Vértice

- **Contextualización del caso:**

El 4 de octubre de 2015 se llevó a cabo una operación antiterrorista coordinada entre España y Marruecos, que culminó con la detención de una célula yihadista dedicada a la captación de mujeres jóvenes con fines de radicalización, adoctrinamiento y favorecimiento del desplazamiento a la zona de conflicto sirio-iraquí para su integración en la organización terrorista Daesh. Esta operación, conocida como “Operación Vértice”, fue ampliamente difundida en prensa bajo titulares como:

“Juzgan a cuatro yihadistas por captación de mujeres para el EI en internet” (El País, 2018)

- **Análisis de las sentencias:**

La Operación Vértice, fue tramitada bajo el Sumario 8/2016, instruido por el Juzgado Central de Instrucción n.º 5 y finalizó con la Sentencia n.º 33/2018 (SAN 3462/2018) dictada por la Sección Tercera de la Sala de lo Penal de la Audiencia Nacional, con confirmación en casación mediante la STS 750/2019 y su posterior inadmisión de nulidad en ATS 5261/2019.

En dicho caso, se procedió a la detención de una célula del Estado Islámico destinada a la captación de mujeres jóvenes, al objeto de que se convirtieran en mujeres de los “leones del Califato”, los muyahidines que combatían en nombre de la organización terrorista, y procedieran a alumbrar “cachorros”, bebés que siguieran con su estirpe. Entre los detenidos figuran según la Sentencia 33/2018 (El Mundo, 2018):

1. Sanae BOUGHROUM, nacida el 15 de agosto de 1992 en Beni Ammart (Marruecos).
2. Layla HAIRA, nacida el 8 de agosto de 1995 en Mhamid Bouib (Marruecos).
3. Saif Eddine HAIK AANIBA, nacido en 1995 en Badalona (España), y
4. Rabio Miguel MEDEIROS ALMEIDA, nacido en 1985 en Angra (Portugal).

En el marco del Sumario 8/2016 tramitado ante el Juzgado Central de Instrucción nº 5, el uso del Agente Encubierto Informático resultó clave en la obtención de pruebas de alto valor probatorio contra los acusados, particularmente en lo relativo a la captación y adoctrinamiento de mujeres jóvenes para su incorporación al Estado Islámico. A través de las interacciones digitales, y gracias a las facultades conferidas por la LECrim tras la reforma de la LO 13/2015, el AEI tuvo acceso a conversaciones privadas, publicaciones restringidas y conductas en redes sociales que, de otro modo, hubieran permanecido ocultas para las fuerzas de seguridad.

Entre las evidencias más significativas se encuentran las siguientes:

a) Conversaciones mantenidas por las acusadas Sanae y Layla a través de Facebook y WhatsApp, en las que se detecta un proceso de captación progresivo:

Primero se presentaban como interesadas en el islam sin connotaciones extremistas, para luego introducir paulatinamente discursos yihadistas. Un ejemplo ilustrativo lo ofrece Miriam cuando contacta con una joven marroquí a quien le expresa:

Lo que hablamos el otro día, cuando te dije que yo te descubrí desde el primer día y creo que es una señal [...] tengo una amiga mía que

le gusta "eso", y quiere ir allí, quiere lo del Estado Islámico y todo ese rollo y su sueño es poder ir allí. Yo cuando la conocí el año pasado y no sabía que... Me preguntó sobre eso de... el Estado... me preguntó... no me pregunta nada del DAESH. Yo no sé... con ella eso... me preguntó sobre el Estado Islámico. (SAN 3462/2018)

b) Propuesta directa de desplazamiento a Siria:

En una de las interacciones, Sanae ofrece a una joven la posibilidad de integrarse en el Estado Islámico, sugiriéndole viajar en noviembre junto a otra "hermana", momento en que le proporciona incluso indicaciones logísticas y medidas de seguridad sobre cómo realizar el viaje, abrir una cuenta bancaria y evitar la detección policial.

c) Uso de grupos cerrados en WhatsApp:

Las investigadas gestionaban al menos tres grupos con hasta 100 usuarios en los que se difundía contenido ideológico radical, justificando la violencia contra infieles y promoviendo la estricta aplicación de la *sharia*. Estas conversaciones fueron grabadas o almacenadas por el AEI con autorización judicial, conforme a lo dispuesto en los artículos 282 bis 6 y 7 LECrim. Tal y como menciona en las conversaciones mantenidas en dichos grupos habría mujeres, entre ellas menores de edad, de diferentes puntos de la geografía española:

Layla: Hay chicas buenas, incluso españolas que se han convertido al Islam. Hay por ejemplo *firdaws*, y... hay muchas, hay como 100 chicas en el grupo.

B: ¿De tu pueblo?

Layla: No, de diferentes lugares, de Valencia, de Barcelona, Madrid, Ceuta, América. Hay incluso de Estados Unidos.

B: Pero son chicas jóvenes, ¿no?

Layla: Sí, las hay con 12, 13, 14, 15, 16. Y las hay con 30 y 40 años, y solemos aprender cosas juntas, nos hacemos preguntas y comentarios y hacemos juego de preguntas sobre temas de religión.

(SAN 3462/2018)

d) Detección de víctimas captadas:

La interacción entre el AEI y las investigadas permitió identificar al menos tres jóvenes marroquíes que habían sido objeto de adoctrinamiento y cuyo destino final era unirse a las filas del Daesh en Siria. En uno de los casos, la joven fue detenida antes de poder abandonar el territorio español, evitándose así su incorporación a una estructura terrorista internacional.

e) Expresiones literales que evidencian la voluntad delictiva de captación para la integración en organización terrorista:

En mensajes de WhatsApp intervenidos, se recogen frases como: “no le hables de la yihad, déjame a mí llevar su proceso” (STS 750/2019), lo que revela una planificación consciente del adoctrinamiento, graduado y orientado a asegurar la fidelización ideológica de las víctimas, sin levantar sospechas prematuras.

Las pruebas obtenidas no solo fueron admitidas en el proceso, sino que resultó determinante para fundar la convicción judicial sobre la existencia de una estructura organizada de captación terrorista, con una jerarquía interna clara, unos roles diferenciados, y una estrategia digital bien definida.

- **Valoración Jurídica de la medida:**

Con relación a la figura del Agente Encubierto Informático, estas sentencias 33/2018, SAN 3462/2018, STS 750/2019 y ATS 5261/2019 son verdaderamente esclarecedoras en cuanto a los requisitos y obligaciones que se deben cumplir para que su instauración se realice con todas las garantías judiciales, pues en ellas se habla sobre dicha figura en al menos, 28 ocasiones.

En ellas, la Audiencia Nacional deja constancia explícita de que se cumplieron “escrupulosamente todos los requisitos legalmente exigidos” para la intervención del Agente Encubierto Virtual (AEV), cuya autorización fue emitida mediante auto judicial fechado el 4 de febrero de 2015. En dicho auto se autorizó su actividad por un período de seis meses (prorrogable), y se especificó con detalle el protocolo de actuación: creación de un perfil ficticio en la red social Facebook, identidad funcional del agente, identidad del traductor de árabe, prohibición expresa de provocación delictiva, y obligación de remitir mensualmente actas de las interacciones con los investigados.

Los autos judiciales incluyen, además, la obligación de solicitar autorización expresa para aquellas diligencias que implicaran restricciones a derechos fundamentales, como escuchas en las que el agente no participara o grabaciones en espacios íntimos, que deberían cumplirse con todas las garantías que se delimitan en el artículo 282 bis.3 de la LECrim, y fueron incorporadas en el caso con la plena observancia de la legalidad vigente.

En base a su fundamentación, queda perfectamente acreditado que su aplicación se extiende a los delitos de terrorismo enjuiciados, así como cualquier otro que se cometiera a través de medios informáticos o el entorno virtual.

El Tribunal Supremo, en su STS 750/2019, avala expresamente la legalidad de este instrumento, recordando que se trata de un “medio de investigación histórica” que ha sido objeto de regulación normativa para dotarlo de mayor seguridad jurídica. Añade que “el agente encubierto debe actuar bajo control judicial, sin provocar el delito, y su actuación debe ser proporcional, finalista y autorizada previamente” STS 750/2019.

Asimismo, en esta sentencia se recoge que debe existir un auto motivado del Juzgado de Instrucción competente, como así ocurrió en este caso, y que el uso

del AEI es legítimo en investigaciones relacionadas con actividades propias de la delincuencia organizada, tal como establece el artículo 282 bis.1 LECrim.

- **Impacto preventivo y simbólico de la operación:**

Desde una perspectiva operativa y social, la operación tuvo un efecto preventivo indiscutible. Se logró desarticular una red que actuaba desde territorio español, dedicada a la captación de mujeres jóvenes a fin de integrarlas en la organización terrorista Daesh mediante técnicas de adoctrinamiento emocional, discurso religioso manipulador y promesas de pertenencia a una comunidad superior.

Las investigadas mantenían una narrativa constante sobre el deber de emigrar al Califato, glorificaban el papel de la mujer mártir y alentaban a otras jóvenes a unirse a la causa. Con su detención se frenó no solo una cadena de reclutamiento activa, sino que se envió un mensaje claro sobre la capacidad del Estado para actuar preventivamente incluso en los espacios más opacos de internet.

El valor simbólico fue especialmente significativo, ya que se rompió la impunidad de quienes instrumentalizaban su género y religión como vehículo de captación terrorista, y se consolidó el papel del AEI como figura clave en la defensa de la seguridad nacional sin renunciar a las garantías del Estado de Derecho.

- **Conclusión:**

En dicho procedimiento judicial la figura del Agente Encubierto Informático se reveló como una herramienta investigativa no solo plenamente legítima, sino también indispensable. Su actuación fue debidamente autorizada conforme a los requisitos formales y materiales exigidos por el artículo 282 bis de la Ley de Enjuiciamiento Criminal, y su validez fue refrendada tanto por la Audiencia Nacional como por el Tribunal Supremo en sede de recurso de casación. La intervención del AEI respetó escrupulosamente los principios de legalidad, necesidad y proporcionalidad, convirtiéndose en elemento clave para la acreditación de los delitos de captación y adoctrinamiento terrorista.

Lejos de cualquier atisbo de provocación, la prueba obtenida evidenció una revelación espontánea y voluntaria de la actividad delictiva por parte de las acusadas, lo que refuerza la solidez probatoria de la operación y su compatibilidad con los derechos fundamentales. La figura del AEI no solo permitió documentar conductas ilícitas en tiempo real, sino también desarticular un entramado de radicalización dirigido específicamente a mujeres jóvenes, muchas de ellas vulnerables, con el riesgo añadido de su desplazamiento a zonas de conflicto, en donde muy probablemente habrían acabado perdiendo la vida.

En consecuencia, este caso representa un precedente paradigmático del correcto uso del agente encubierto digital como medida de investigación judicialmente tutelada, alineada con la doctrina constitucional y la jurisprudencia consolidada del Tribunal Supremo. Se confirma así la plena idoneidad jurídica, operativa y ética del AEI como recurso estratégico en la lucha contra el terrorismo de corte yihadista en el entorno virtual.

12.2.3. SAN 3070/2019 y STS 3249/2021

- **Contextualización del caso:**

El 28 de septiembre de 2016 se llevó a cabo una operación antiterrorista internacional coordinada entre España, Bélgica y Alemania, bajo la supervisión del Juzgado Central de Instrucción nº 5 de la Audiencia Nacional. La operación permitió la detención de cinco personas en diferentes países europeos, acusadas de formar parte de una estructura yihadista activa, plenamente alineada con el ideario de Daesh. La célula operaba a través de redes sociales, especialmente la página de Facebook “Islam en Español”, con más de 32.500 seguidores, utilizada como vehículo de adoctrinamiento, captación y propaganda de terrorismo, hechos que le transfirieron un gran impacto mediático:

“Tres presuntos yihadistas del Estado Islámico detenidos en Barcelona y Melilla” (EL Confidencial, 2018).

“2La célula yihadista desarticulada hoy en España, Bélgica y Alemania representaba una amenaza grave, concreta y continuada para la seguridad en Europa” (La Moncloa, 2018).

- **Análisis de las sentencias:**

La desarticulación de esta célula yihadista transnacional, enmarcada en las Diligencias Previas 124/15 del Juzgado Central de Instrucción nº 5, culminó en las sentencias SAN 3070/2019 de la Audiencia Nacional y STS 3249/2021 del Tribunal Supremo. La investigación judicial, de amplio alcance y con colaboración internacional, acreditó la existencia de una organización con clara vocación propagandística y captadora, cuyos integrantes desarrollaban sus funciones desde España, Bélgica y Alemania.

Según la nota oficial del Ministerio del Interior, los acusados utilizaban la página de Facebook “Islam en Español” como vehículo de difusión ideológica:

Bajo el pretexto de divulgar contenido religioso, en la misma página web se intercalaban mensajes y comentarios de carácter radical en los que se ensalzaban a los combatientes yihadistas ‘mártires’, las acciones llevadas a cabo por el DAESH y la importancia de la Yihad individual. (Ministerio del Interior, 2016)

Esta plataforma, con más de 32.000 seguidores, era administrada por algunos de los detenidos, entre ellos Aziz Mezroui Ramdani, Junaid Hameed Parveen y Abdellah Athanouti Mohamed. La página albergaba desde vídeos de ejecuciones yihadistas hasta manuales operativos e instrucciones sobre desplazamiento a zona de combate (El Mundo, 2016).

El Agente Encubierto Informático (AEI) desempeñó un papel crucial en esta investigación, facilitando la obtención de pruebas que permitieron acreditar la existencia de una estructura jerarquizada dedicada a la radicalización y al fomento del terrorismo yihadista. Tal y como recoge la SAN 3070/2019, gracias a la interacción encubierta se pudo constatar que los miembros del grupo:

- Reproducían y compartían mensajes en los que se “llamaba a la guerra santa y a la destrucción del enemigo infiel”.
- Animaban a otras personas a viajar a Siria, proporcionándoles pautas para no levantar sospechas, como el uso de identidades falsas y rutas seguras.
- Gestionaban grupos privados de difusión yihadista en redes sociales y servicios de mensajería cifrada.
- Compartían vídeos oficiales de la propaganda de Daesh y animaban a visualizar los asesinatos cometidos a los infieles, demostrando una glorificación sistemática del terror.

Entre los contenidos intervenidos destacan conversaciones en las que los acusados afirmaban: “El mártir alcanza el paraíso sin juicio” y “morir matando es el mayor honor que puede alcanzar un musulmán”. Conversaciones y contenidos a los que no se hubiera podido tener acceso sin autorización judicial expresa del AEI, al amparo del artículo 282 bis de la L.O 13/2015. Así entre los ingentes comentarios y difusiones recabados por el Agente Encubierto Informático entre los más de 106 folios de sentencia, se destacan numerosas incitaciones a la yihad, vanagloria de los líderes de Daesh y Al-Qaeda, amenazas explícitas a Francia y Al-Andalus, así como una justificación monotemática de la ascensión al Paraíso y sus beneficios celestiales si mueres como mártir en la senda de Allah:

El día 4 de mayo de 2016 [Contenido recogido en el Acta Web nº

NUM081 del Agente Encubierto Informático Judicializado, folio 266 de la Pieza separada], el investigado publicó una imagen firmada con su seudónimo “#Zeref en la página que administraba “islam en Español”. En la misma se observa una pareja vestida con ropa musulmana con la frase “Todo musulmán está dispuesto a morir por su religión”, acompañada de la fotografía de unos leones con la frase “Igual a los leones están dispuestos a morir por su manada”. (SAN 3070/2019).

“El día 18 de julio de 2016 [Contenido recogido en el Acta Web nº NUM103 del Agente Encubierto Informático Judicializado, folio nº 844], el procesado difundió en su perfil " Abu Khatab " un vídeo titulado: "Mensaje del Estado Islámico a los franceses". En el mismo se puede ver a un miembro del grupo terrorista DAESH lanzando unas soflamas: "Tengo un mensaje para el pueblo democrático, para el pueblo infiel. Vosotros los europeos, vosotros occidentales, vosotros que queréis la democracia y la laicidad en el mundo árabe, seguid el ejemplo del pueblo español en 2004. Ellos (los españoles) fueron asesinados en su propia tierra por los muyahidines. Y entonces el pueblo español salió a la calle apelando a la dimisión de su gobierno (...). ¡Salid y decidles perros! Decidles que dimitan porque su política exterior no hizo más que asesinaros poco a poco. Sabed que los creyentes tienen un dogma y ese dogma es que, si vosotros matáis a los musulmanes, nosotros matamos a los infieles y será en vuestra tierra.

(SAN 3070/2019)

En relación con el Agente Encubierto Informático la STS 3249/2021 confirmó la legalidad y legitimidad de la actuación policial y judicial. En concreto, validó la intervención del AEI por haberse realizado con autorización judicial expresa, de forma proporcionada y sin inducir en ningún momento la comisión del delito, ajustándose así al artículo 282 bis de la LECrim. El Supremo señala que “la prueba obtenida mediante la interacción del agente encubierto virtual se ha revelado como

decisiva para esclarecer los hechos, sin que exista viso de provocación o extralimitación”.

En suma, las sentencias ratifican que esta célula operaba conforme a la estrategia mediática del DAESH, reproduciendo su propaganda en castellano, captando jóvenes hispanohablantes y proponiendo su integración operativa mediante el desplazamiento a zonas de conflicto.

- **Valoración jurídica de la medida:**

Ambas resoluciones judiciales avalan la legitimidad de la intervención del Agente Encubierto Informático. En particular, la STS 3249/2021 recuerda:

La actividad encubierta fue autorizada de forma previa por el juez instructor, y los agentes actuaron con pleno respeto a los límites legales establecidos. No hubo provocación del delito, sino una recopilación de prueba derivada de la propia iniciativa delictiva de los acusados. (STS 3249/2021, p. 14)

El uso del AEI fue proporcional y ajustado al principio de subsidiariedad, al tratarse de una red criminal transnacional con potencial de provocar graves daños.

- **Impacto preventivo y simbólico de la operación:**

Desde el punto de vista operativo y social, la desarticulación de esta célula yihadista internacional activa en España, Bélgica y Alemania, tuvo un impacto preventivo de especial relevancia para la seguridad nacional y europea. Los miembros del grupo habían desarrollado una infraestructura digital estable y altamente profesionalizada, orientada a la difusión masiva de contenidos pro-Daesh en lengua española, con el fin de captar a jóvenes musulmanes hispanohablantes y dirigirlos hacia la radicalización y, en última instancia, al desplazamiento a zonas de conflicto.

La neutralización de esta red, cuya página principal ("Islam en Español") contaba con más de 32.500 seguidores y crecía a un ritmo de 500 nuevas

incorporaciones semanales, impidió la consolidación de un aparato ideológico y logístico con capacidad para alimentar otras células en Europa y Latinoamérica. La incautación de dispositivos, manuales operativos, vídeos de extrema crueldad, y el acceso a las conversaciones interceptadas por el Agente Encubierto Informático (AEI) permitieron no solo documentar la actividad delictiva, sino detener su expansión.

Tal como recoge el Ministerio del Interior: “la célula desarticulada representaba una amenaza grave, concreta y continuada para la seguridad de las sociedades occidentales” (Ministerio del Interior, 2016).

Desde una perspectiva simbólica, esta operación demostró la capacidad del Estado español para actuar coordinadamente a nivel internacional frente a redes descentralizadas pero interconectadas, que aprovechaban el vacío idiomático y doctrinal en español para establecer una narrativa yihadista propia.

- **Conclusión:**

A la luz del análisis conjunto de la Sentencia 3070/2019 de la Audiencia Nacional y su confirmación en la STS 3249/2021 del Tribunal Supremo, resulta incuestionable la plena validez jurídica y operativa del uso del Agente Encubierto Informático en el desarrollo de la investigación. Su actuación no solo fue formalmente autorizada por auto judicial conforme al artículo 282 bis de la LECrim, sino que también estuvo sujeta a los principios de proporcionalidad, necesidad, legalidad y subsidiariedad, tal como exige la jurisprudencia consolidada del alto tribunal.

El agente encubierto accedió a la comunidad yihadista virtual bajo identidad simulada, en entornos cerrados y moderados por los acusados, logrando documentar en tiempo real las interacciones delictivas vinculadas con el adoctrinamiento, captación y difusión de contenidos violentos, así como la transmisión de mensajes estratégicos de Daesh orientados a generar una red propagandística estable en lengua española. En sus intervenciones quedaron recogidas expresiones radicales, publicaciones apologéticas, así como conversaciones privadas que evidenciaban la existencia de vínculos directos con estructuras operativas de la organización terrorista.

La cadena de custodia digital, la autoría funcional del agente, y el carácter espontáneo y no inducido de las manifestaciones de los acusados permitieron que la prueba fuera plenamente admisible, tanto en fase de instrucción como en juicio oral. Así lo ratificó el Tribunal Supremo, que refrendó que no existió provocación, sino una revelación voluntaria de la conducta criminal por parte de los investigados.

En este sentido, las sentencias dejan constancia de que la página "Islam en Español" gestionada por los condenados desde España, Bélgica y Alemania, fue un vehículo clave para la expansión del ideario terrorista, el reclutamiento de jóvenes musulmanes hispanohablantes y el eventual traslado de combatientes a zona de conflicto. La intervención del AEI permitió monitorizar y registrar este proceso desde su fase inicial, asegurando la intervención temprana de las autoridades y evitando consecuencias irreversibles.

Por todo ello, el uso del Agente Encubierto Informático en este caso constituye un ejemplo paradigmático de técnica de investigación jurídicamente válida y operacionalmente eficaz, imprescindible para dismantelar amenazas complejas, transnacionales y tecnológicamente sofisticadas como las del terrorismo yihadista digital.

12.2.4. SAN 5421/2018 y SAN 1447/2019. Operación Silicon

- **Contextualización del caso:**

El 26 de julio de 2017, el Ministerio del Interior informó públicamente de la detención en la localidad vizcaína de Balmaseda de Yassin I., un joven de 22 años y nacionalidad marroquí, por realizar tareas de difusión intensiva de propaganda yihadista a través de Internet, especialmente vinculada al grupo terrorista Daesh.

Según indicó el Gobierno español, el detenido procedía de una familia radicalizada de origen marroquí y se encontraba "en una fase avanzada de radicalización a la vez que mantenía de forma permanente contacto con combatientes yihadistas en Siria (Noticias de Gipuzkoa, 2017)", y había asumido como propia la ideología de Daesh, dedicándose a la justificación pública del

terrorismo, glorificación de sus mártires, difusión de manuales de combate y captación de nuevos seguidores.

Entre los titulares de prensa más destacados sobre el caso:

“Detenido en Vizcaya un marroquí de 22 años por difundir en internet la ideología del grupo terrorista Daesh” (La Moncloa, 2017)

“Detenido en Balmaseda por apoyar al ISIS, un joven de 22 años” (EiTB, 2017)

“El detenido en Balmaseda vivía en un entorno radical” (Noticias de Gipuzkoa, 2017)

- **Análisis de las sentencias:**

La operación Silicon, llevada a cabo por la Jefatura de Información de la Guardia Civil, en concordancia con el Servicio de Información de la Comandancia de Vizcaya, y apoyados por el Servicio de Información de Murcia, fue judicialmente tramitada bajo Diligencias Previas n.º 63/2017 por el Juzgado Central de Instrucción n.º 3, y culminó en la sentencia SAN 5421/2018, dictada por la Sección Primera de la Sala de lo Penal de la Audiencia Nacional, ratificada posteriormente por SAN 1447/2019.

En los hechos probados se describe con claridad la actividad desarrollada por el acusado:

- Administraba cuentas de YouTube, Facebook y Google Plus bajo seudónimos y perfiles islamistas.
- Difundía contenido de “extrema violencia”, vídeos oficiales del Estado Islámico, imágenes de ejecuciones, y manuales de fabricación de explosivos.
- Justificaba explícitamente atentados cometidos por Daesh en Europa, incluyendo las acciones en París, Bruselas o Berlín.
- Interactuaba con otros usuarios compartiendo mensajes como: “La yihad es el camino de la verdad. Occidente será derrotado”.

En dicha operación, la figura del Agente Encubierto Informático (AEI) resultó determinante desde el punto de vista jurídico-procesal y operativo. Su intervención permitió salvar uno de los principales obstáculos en la investigación, el acceso lícito

y controlado al entorno privado del investigado, que mantenía cifrado deliberadamente para eludir la acción de las fuerzas de seguridad.

El investigado, Yassin I., utilizaba herramientas de anonimización como redes privadas virtuales (VPN), navegadores tipo TOR y plataformas de mensajería cifrada para difundir propaganda yihadista sin revelar su identidad real. Estas precauciones dificultaban una identificación directa y evidenciaban su conocimiento avanzado del ecosistema digital, que posteriormente se demostró que se debía a sus amplios conocimientos en informática.

La actuación encubierta, debidamente autorizada por auto judicial conforme al artículo 282 bis de la LECrim, permitió la creación de una identidad ficticia funcional, con la que el AEI logró entablar una relación digital sostenida con el acusado, obteniendo acceso a grupos cerrados, conversaciones privadas y canales restringidos. En esas interacciones, Yassin I. compartió contenidos que evidenciaban su plena adscripción al ideario del Estado Islámico (Daesh), tales como vídeos de ejecuciones, manuales de adoctrinamiento, imágenes de mártires y proclamas contra Occidente.

Entre los ejemplos extraídos de la sentencia SAN 1447/2019 se encuentran reiteradas alusiones y fotografías del ideólogo de Al-Qaeda Osama Bin Laden, junto al comentario: “nosotros venceremos con cajas de munición y no con urnas, ni con su supuesta democracia”. Así como amenazas a occidente y la comunidad internacional:

¡Oh cristianos, chiitas, laicos, apostatas, judíos y a todos los héroes en su totalidad! Aliaros contra los musulmanes todo lo que queráis aliaros, trampear contra ellos todo lo que os plazca, ardid argucias y engañar y avituallaros. No obstante, seréis vencidos y en el infierno introducidos. Cristianos seréis vencidos, chiitas seréis vencidos, apostatas seréis vencidos, judíos seréis vencidos [...] Estamos en guerra, y todo musulmán debe apoyar a sus hermanos combatientes. El Estado Islámico traerá justicia

a los infieles [...] La yihad es un deber de todo creyente. Daesh no es terrorismo, es el ejército del califato. (SAN 1447/2019)

Además de ello, ostentaba una clara justificación a la comisión de atentados terroristas como el del 11-S y otros, destacándose la publicación que realizó minutos más tarde del atentado de Berlín el 19 de diciembre del 2016, en el que un yihadista de Daesh realizó un atropello masivo en un mercadillo navideño con un camión de grandes toneladas, y en donde Yassin, expresaba: “Allah es el más grande, Allah es el más grande, Allah es el más grande. Este (en referencia al atentado) es un hecho que destapa las contradicciones de todos los mudéjares y sus seguidores” (SAN 1447/2019).

Además, se detectó que el acusado administraba perfiles secundarios y compartía enlaces a plataformas espejo de Al-Hayat Media Center y otros canales oficiales de Daesh, dificultando su rastreo.

Estas pruebas no sólo fueron obtenidas sin inducir a la comisión del delito, sino que revelaron una actividad delictiva preexistente, lo que refuerza su valor probatorio conforme a la jurisprudencia del Tribunal Supremo.

- **Valoración jurídica de la medida:**

La aportación probatoria del Agente Encubierto Informático (AEI) en la operación SILICON fue esencial no solo en términos de contenido, sino también por el acceso que permitió a un entorno comunicacional cuidadosamente blindado por el acusado. El AEI, debidamente autorizado por sucesivos autos judiciales, “consiguió infiltrarse en la cuenta de Facebook del investigado, configurada como privada desde noviembre de 2015, siendo aceptado como amigo en mayo de 2017. A través de esta vía, y gracias a la simulación de afinidad ideológica con el ideario yihadista, se obtuvieron elementos de prueba de alto valor jurídico, incluyendo imágenes, mensajes y enlaces alojados en páginas de acceso restringido que evidenciaban sin ambigüedad el alineamiento del acusado con el grupo terrorista Daesh (SAN 5421/2018, SAN 1447/2019).

Entre los contenidos recuperados destacan publicaciones con iconografía yihadista, manuales operativos, enlaces a portales cifrados, como el servidor ruso mail.ru, utilizado por el acusado para almacenar material propagandístico radical sin dejar trazabilidad de sus comunicaciones, así como un manual táctico para la realización de atentados terroristas con estrategias de guerrilla en entornos urbanos. De forma reveladora, durante una breve interrupción del uso de software de anonimización VPN, se pudo rastrear su actividad digital, constatando la descarga de archivos producidos por agencias mediáticas del Estado Islámico como Amar o Ajnad Media.

En paralelo, el análisis del dispositivo móvil de Yassin I. reveló archivos multimedia radicales, cánticos bélicos (*nasheed*) e infografías de combate, así como indicios técnicos que confirmaban la utilización de redes privadas virtuales para ocultarse y aplicaciones para burlar la censura geográfica, consolidando su perfil de actor radicalizado y operativo.

Por tanto, las interacciones mantenidas por el AEI no fueron un simple canal de observación pasiva, sino un vector de acceso estratégico que permitió sustanciar acusaciones de autoadocctrinamiento, apología del terrorismo y difusión de contenido destinado a incitar a la violencia, conforme al art. 578 del Código Penal.

- **Impacto preventivo y simbólico de la operación:**

Desde una perspectiva operativa, la Operación Silicon permitió neutralizar la evolución en la radicalización de un sujeto que, aunque no había alcanzado la fase ejecutiva de un atentado, se encontraba plenamente inmerso en la apología del terrorismo, el consumo de propaganda oficial de Daesh y la reiterada incitación a la violencia religiosa contra los infieles.

El acusado, Yassin I., actuaba de forma constante en redes sociales, utilizaba sistemas de cifrado, ocultación de IP y dispositivos tecnológicos que dificultaban su rastreo. Su actividad no solo implicaba un riesgo abstracto, sino que, tal como recoge la sentencia, mantenía contacto regular con otros individuos afines y terroristas ya enrolados en Daesh, mostrando claramente una evolución doctrinal hacia posiciones de martirio y lucha armada. El entorno digital en el que se movía representaba un espacio de difícil penetración sin la cobertura proporcionada por

el Agente Encubierto Informático, quien accedió a sus entornos privados bajo identidad simulada, obteniendo prueba anticipada de su peligrosidad.

Desde el plano preventivo, el valor de esta operación radica en su capacidad para interrumpir precozmente un proceso de radicalización violenta, evitando que cristalizara en una amenaza directa contra la seguridad ciudadana. En este sentido, la actuación encubierta permitió trasladar la actividad delictiva desde un plano abstracto (simpatía ideológica) a un plano penalmente relevante (glorificación y justificación del terrorismo, posesión de manuales y vídeos doctrinales, etc.), legitimando la intervención judicial.

En términos simbólicos, la operación tuvo especial repercusión mediática, no solo por la juventud del detenido y su arraigo en España, sino también porque reveló una contradicción social significativa: el investigado recibía ayudas públicas del Estado español mientras simultáneamente promovía el ideario del Daesh en redes sociales contra el Estado español. Este dato, ampliamente recogido por medios de comunicación como *El Confidencial* o *Intereconomía* (2017), generó un debate público relevante sobre la necesidad de reforzar los mecanismos de control y prevención del extremismo digital, especialmente entre jóvenes en situación de exclusión o vulnerabilidad social.

Asimismo, el mensaje institucional fue claro: la actuación del Estado no se limita a la reacción tras un atentado, sino que se adelanta al riesgo, se infiltra en los entornos virtuales y desarticula las redes propagandísticas antes de que éstas germinen en violencia física.

- **Conclusión:**

La actuación del Agente Encubierto Informático en la Operación Silicon fue plenamente ajustada a Derecho, conforme a los artículos 282 bis y siguientes de la Ley de Enjuiciamiento Criminal, y resultó indispensable para acreditar la conducta delictiva del acusado. A través de interacciones digitales en entornos cerrados, el AEI obtuvo pruebas lícitas, no provocadas, que permitieron documentar la adhesión ideológica de Yassin I. al Estado Islámico, su papel como difusor de propaganda yihadista, y su exaltación constante de atentados terroristas recientes.

La validez jurídica de las pruebas fue ratificada en las SAN 5421/2018 y SAN 1447/2019, que reconocieron expresamente que la investigación fue desarrollada con todas las garantías procesales, sin extralimitación ni vulneración de derechos fundamentales. El valor probatorio de las actas del AEI y del contenido intervenido fue incuestionable y se constituyó en base probatoria suficiente para sostener la condena.

Este caso constituye un ejemplo paradigmático de cómo el Estado puede actuar con eficacia frente a amenazas solitarias, ideológicamente radicalizadas, mediante instrumentos legales de vanguardia. La operación no solo impidió la consolidación de una red de propaganda pro-Daesh en el País Vasco, sino que dejó patente la relevancia de anticiparse a la fase ejecutiva del delito mediante mecanismos de detección temprana, vigilancia digital y prueba encubierta debidamente autorizada.

12.2.5. SAN 3054/2018 y STS 934/2019. Operación Talibán

- **Contextualización:**

El 23 de febrero de 2016 se ejecutó en la ciudad autónoma de Ceuta una operación antiterrorista que culminó con la detención de cuatro individuos acusados de formar parte de una célula yihadista activa, cuya principal misión era la captación y adoctrinamiento de jóvenes y menores para su incorporación al Estado Islámico (Daesh). La operación, coordinada por el Juzgado Central de Instrucción n.º 5 de la Audiencia Nacional bajo la dirección del magistrado José de la Mata, fue bautizada mediáticamente como “Operación Talibán”, debido al carácter ultraconservador, ortodoxo y doctrinario del grupo desarticulado, con fuerte inspiración en el salafismo yihadista.

Los arrestados fueron identificados como Rhimou Bghil Abdesalam, Ilias Mohamed Mohamed, Hakkin Monerris y Fuad Makhoulf Iabbassane. Según fuentes del Ministerio del Interior, los tres primeros fueron ingresados en prisión provisional por delitos de integración en organización terrorista, adoctrinamiento y enaltecimiento del terrorismo, mientras que el cuarto fue puesto en libertad por no hallarse indicios suficientes en su contra en ese momento inicial de la instrucción (Europa Press, 2016; El Pueblo de Ceuta, 2016).

La célula actuaba desde el barrio del Príncipe Alfonso, zona históricamente vinculada a procesos de radicalización, exclusión social y conflictividad religiosa. El grupo, según la investigación, presentaba una estructura interna definida y estable, distribuía tareas y adoptaba avanzadas medidas de seguridad, tanto físicas como virtuales, para evitar su detección. Su actividad no era improvisada ni reactiva, sino sistemática, planificada y alineada con las directrices doctrinales del Estado Islámico, en particular las relacionadas con la creación de los llamados cachorros del Califato: niños y adolescentes captados, deshumanizados y convertidos en combatientes tras procesos de adoctrinamiento progresivo (Ministerio del Interior, 2016).

Uno de los elementos más relevantes del caso fue el perfil de Rhimou Bghil Abdesalam, joven ceutí de 18 años que había intentado cruzar la frontera entre Turquía y Siria para unirse al DAESH, siendo interceptada por las autoridades turcas en enero de 2015. Su figura adquirió notoriedad pública tras conocerse que se encontraba en proceso de radicalización desde al menos un año antes, bajo influencia familiar y religiosa, y que mantenía vínculos ideológicos con combatientes fallecidos en Siria. Tras ser repatriada a España, continuó desarrollando labores activas de captación entre menores de su entorno, configurándose como referente femenino del yihadismo local en Ceuta (El Mundo, 2015).

Según las fuentes policiales, la célula mantenía contacto directo y constante con combatientes del Estado Islámico en zona de conflicto, quienes los instruían sobre metodologías de captación, propaganda y compartimentación operativa. El grupo había comenzado a elaborar planes para exportar su modelo de captación a otros países europeos, estableciendo células hermanas que replicaran la experiencia ceutí, considerada por DAESH como un modelo funcional de reclutamiento en contexto urbano marginal (Europa Press, 2016).

La peligrosidad del entramado radicaba, precisamente, en su doble capacidad: por un lado, ejercer una influencia directa sobre jóvenes emocionalmente vulnerables; por otro, funcionar como plataforma de legitimación y glorificación del ideario yihadista, alimentando una narrativa de pertenencia y martirio orientada a la acción.

De entre los rotativos de prensa que se hacían eco de dicha Operación, se destacan:

“La célula yihadista desarticulada en Ceuta centraba su actividad en captar, adoctrinar y enviar a la zona de conflicto sirio-iraquí a jóvenes y a niños para convertirlos en futuros combatientes” (La Moncloa, 2016).

- **Análisis de las sentencias:**

La Audiencia Nacional, en su SAN 3054/2018, condenó a Rhimou Bghil Abdesalam a cinco años de prisión por un delito de integración en organización terrorista, y a Ilias Mohamed Mohamed y Hakkin Monerris por delitos de enaltecimiento del terrorismo y adoctrinamiento. La sentencia fue posteriormente confirmada en casación por el Tribunal Supremo en su STS 934/2019, que ratificó la existencia de una estructura de captación y radicalización plenamente operativa desde el barrio del Príncipe Alfonso, en Ceuta.

Uno de los elementos probatorios más relevantes para sustentar la condena fue la actuación de un Agente Encubierto Informático (AEI) debidamente autorizado por el juez instructor, quien logró infiltrarse en los entornos digitales del grupo y mantener conversaciones directas con los acusados, especialmente con Hakkin Monerris, conocido por su actividad en redes sociales como difusor del ideario yihadista.

En dichas interacciones, el AEI logró establecer contacto con otros miembros del entorno radical, quienes compartían enlaces a vídeos de DAESH, manuales de adoctrinamiento, y mensajes incitadores al odio contra infieles. En otra conversación, Hakkin Monerris remitió al AEI un vídeo de ejecuciones comentado con la frase: “esto no es violencia, es justicia divina. Así tratan a los enemigos del islam los verdaderos creyentes” (SAN 3054/2018).

Así mismo, las sentencias están repletas de conversaciones entre el AEI y los encausados, que evidenciaban los contactos que mantenían con el conglomerado terrorista que operaba en la zona de conflicto sirio-iraquí, entre las que se destacan:

AEI: Me dijo [alias: Chillon] que ya intentaste ir y q tuviste algún problema, eso me lo tienes q contar para aprender.

Rhimou Bghil: Si, eso fue la falta de preparación, no sabía bien el camino, y nadie me indicó como hacerlo", [...] "Fui por casa blanca y de ahí cojo un avión a Turquía y de Turquía a un pueblo llamado Gaziantep". "En verdad fue por falta de organización"... Prefiero irme con Jabhat Al Nusra (filiar de Al-Qaeda), aunque todos los contactos que tengo son de Dawla al Islamiya (Daesh). STS 3054/2018)

Nuevamente, en otra conversación mantenida entre Rhimou y el AEI el 20 de octubre de 2016, le indica al AEI que su hermano también emigró a la yihad Siria y tiene contacto con combatientes:

Los contactos que tengo son del Dawla al Islamiya (Daesh), conozco a Abu Omar Al Silari (combatiente yihadista identificado en la causa). Hablé con el hermano, lo conozco por las redes sociales porque mi hermano estuvo ahí hace un par de años. (STS 3054/2018)

Además, la SAN 3054/2018 acreditó la existencia de perfiles cerrados en redes sociales, en los que se compartía contenido yihadista, se reproducían cánticos *nasheed*, y se exaltaba la figura del mártir. En uno de estos espacios digitales, gestionado por Ilias Mohamed, se compartió el siguiente mensaje: "La bandera nos ha llamado para iluminar el camino del destino. Para librar la guerra contra el enemigo. Todo Aquel que entre nosotros muere, en sacrificio por la defensa, disfrutará de la eternidad en el paraíso. Mañana partirá" (SAN 3054/2018, p. 13).

En suma, la SAN 3054/2018 y la STS 934/2019 constituyen un doble referente jurisprudencial sobre la validez de la figura del AEI en la persecución del terrorismo de corte yihadista, y especialmente en contextos donde el adoctrinamiento se produce de manera emocional, digital y colectiva, bajo la cobertura de referentes locales con fuerte ascendencia social.

- **Valoración jurídica de la medida:**

Desde la perspectiva jurídico-procesal, la intervención del Agente Encubierto Informático (AEI) en la Operación Talibán se ajustó con plena escrupulosidad a lo establecido en el artículo 282 bis de la Ley de Enjuiciamiento Criminal (LECrim), introducido por la Ley Orgánica 13/2015. Esta norma habilita la autorización judicial previa para que un funcionario de policía judicial actúe bajo identidad encubierta en entornos digitales, con el fin de detectar, documentar y prevenir delitos especialmente graves, como los contemplados en el artículo 573 y siguientes del Código Penal relativos al terrorismo.

En el caso que nos ocupa, las conversaciones digitales mantenidas por el AEI con los acusados, especialmente con Hakkin Monerris y con Rhimou Bghil, sirvieron para documentar, sin ningún tipo de inducción ni provocación, manifestaciones espontáneas de glorificación del terrorismo, alineamiento ideológico con el Estado Islámico y predisposición a participar en acciones violentas. La Audiencia Nacional reconoció expresamente la validez probatoria de estas interacciones, subrayando que el Instructor de las diligencias:

Detectó la preocupación de aquella por el retorno a Siria, por lo que se le propuso a la autoridad judicial la intervención de un agente encubierto informático (AEI), el cual contactó con una terrorista de la zona de Siria que a su vez facilitó el teléfono de dicho agente a la acusada, momento en que se comprobó que se trataba de Rhimou [...] una mujer que entró en contacto con el Agente Encubierto Informático (AEI), cuya intervención estaba autorizada judicialmente en pieza separada. El contacto entre el AEI y la

mujer se produjo por primera vez el 6 de julio de 2016, con la finalidad de captar al AEI e instarle a que le acompañase a ella en su próximo desplazamiento a territorio sirio. (SAN 3054/2018, p. 17)

Asimismo, el Tribunal Supremo enfatiza en su STS 934/2019 que la actividad del AEI se enmarcó dentro de los principios de legalidad, necesidad, proporcionalidad y subsidiariedad, los cuales constituyen garantías fundamentales cuando se trata de medidas restrictivas de derechos. En este sentido, no se trató de una actuación prospectiva sin control, sino de una acción específica contra personas ya señaladas por su conducta reiterada de difusión de contenidos yihadistas. A la vez que recuerda que la actuación encubierta está amparada en derecho cuando existe una resolución judicial motivada, con delimitación de alcance, duración y condiciones, como fue el caso. La infiltración del AEI en los entornos digitales cerrados del acusado permitió acceder a comunicaciones relevantes para la causa, cuya autenticidad, contexto y contenido fueron analizados pericialmente por expertos policiales y ratificados durante el juicio oral.

A su vez, conviene destacar que esta jurisprudencia no solo legitima la intervención encubierta, sino que refuerza la doctrina consolidada sobre la admisibilidad de la prueba digital obtenida mediante identidad simulada, siempre que no exista provocación, como también ha señalado el Tribunal Constitucional (STC 197/2009 y STC 127/2020), en base a legalidad que otorga el artículo 282 bis de la LECrim.

- **Impacto preventivo y simbólico de la operación:**

Desde una perspectiva preventiva, la Operación Talibán constituyó un hito significativo en la lucha contra el terrorismo yihadista en territorio español, al poner de manifiesto que los procesos de captación y adoctrinamiento no se limitaban a estructuras jerárquicas clásicas ni a canales virtuales lejanos, sino que también se desarrollaban de forma arraigada, constante y silenciosa desde entornos barriales vulnerables como el del Príncipe Alfonso, en Ceuta.

El desmantelamiento de esta célula impidió que continuase una estrategia de reclutamiento que ya había comenzado a dar frutos. La interceptación de Rhimou Bghil Abdesalam en la frontera turco-siria fue decisiva, pues de haberse consumado su incorporación a las filas del Estado Islámico, se habría producido una legitimación simbólica de la célula, generando un efecto llamado especialmente potente entre jóvenes ceutíes. La reacción institucional rápida, coordinada y técnicamente fundamentada consiguió cortar de raíz un proceso de radicalización que había alcanzado un nivel avanzado y orientado hacia la acción (Europa Press, 2016; El País, 2016).

Además, el uso de técnicas encubiertas digitales, a través del Agente Encubierto Informático, permitió penetrar en entornos cerrados, virtuales y altamente compartimentados que eran inaccesibles por métodos tradicionales. El acceso a estos canales no sólo ofreció evidencia probatoria anticipada, sino que permitió identificar dinámicas de captación emocional, conversaciones de glorificación del martirio y mensajes de aliento al desplazamiento a zona de combate. Esto reforzó la hipótesis, ya advertida por el Centro de Inteligencia contra el Terrorismo y el Crimen Organizado (CITCO, 2025), de que la proximidad emocional, el liderazgo de iguales y la normalización del extremismo religioso son los principales vectores de entrada al yihadismo para los adolescentes en contextos marginales.

En el plano simbólico, el caso tuvo una enorme repercusión mediática y social. La imagen de una joven ceutí, menor de edad en el momento en que inició su radicalización, que posteriormente se convirtió en referente de una red de captación, trastocó los marcos clásicos de percepción del terrorismo, habitualmente asociados a hombres adultos y estructuras jerarquizadas. Esta transformación del perfil del captador, cada vez más joven, local y doctrinalmente preparado, obligó a replantear las estrategias de prevención, incluyendo nuevas metodologías de vigilancia digital, educación resiliente en comunidades vulnerables, y programas de detección precoz.

Asimismo, el caso generó un debate público relevante sobre la instrumentalización del género por parte del Estado Islámico. Rhimou, al igual que otras mujeres implicadas en causas similares, no desempeñaba un papel pasivo, sino activo, como canalizadora de doctrina, reclutadora emocional y agente de legitimación religiosa. Su conducta desbarató el imaginario tradicional de la mujer

radicalizada como víctima, y evidenció la capacidad del aparato yihadista para transformar referentes femeninos en elementos funcionales del engranaje terrorista, con el agravante añadido de su potencial para captar a otras jóvenes mediante afinidad identitaria.

En definitiva, la Operación Talibán no solo neutralizó una célula de riesgo real, sino que ofreció una lección operativa y doctrinal sobre la evolución del fenómeno yihadista en clave local a través de la feminización del reclutamiento, penetración en entornos juveniles, expansión por redes sociales y canales de mensajería cifrados, en este caso Whatsapp, y adaptación al lenguaje y a la vulnerabilidad emocional del entorno. Todo ello fue posible gracias a un enfoque de investigación integral, en el que confluyeron medios procesales novedosos, como el AEI, la obtención de inteligencia y pruebas fehacientes a través de la interacción con humanos (Humint), y la tutela judicial efectiva que permitió actuar dentro del marco garantista del Estado de Derecho.

- **Conclusión:**

La Operación Talibán representa un paradigma operativo y jurisprudencial en el empleo de técnicas de investigación encubierta en el ámbito del terrorismo yihadista. Su análisis permite extraer enseñanzas fundamentales sobre el modo en que el fenómeno de la radicalización violenta puede manifestarse en contextos sociales próximos, utilizando canales digitales opacos y liderazgos emergentes de fuerte carga emocional e identitaria.

La intervención del Agente Encubierto Informático (AEI) resultó determinante para acreditar las actividades ilícitas de los acusados, particularmente en lo relativo a las metodologías de atracción y favorecimiento del desplazamiento a zona de conflicto de los captados que ya tenían probada su eficacia en connivencia con muyahidines de Daesh ya desplazados a la zona de conflicto siria, así como mensajes y soflamas destinados a la glorificación del terrorismo, el adoctrinamiento y la predisposición al desplazamiento a zona de conflicto. Su actuación, debidamente autorizada conforme a los requisitos legales establecidos en el artículo 282 bis de la Ley de Enjuiciamiento Criminal, y ratificada tanto por la Audiencia Nacional como por el Tribunal Supremo, fue ajustada a

Derecho, respetando los principios de legalidad, necesidad, proporcionalidad y ausencia de provocación.

Desde un punto de vista sustantivo, el caso evidencia que las dinámicas de captación y adoctrinamiento pueden desarrollarse en ámbitos locales, mediante figuras aparentemente marginales, pero doctrinalmente activas, capaces de generar entornos de radicalización emocional en menores de edad. El uso de referentes femeninos en tareas de legitimación y adoctrinamiento, como en el caso de Rhimou Bghil, constituye un indicador de la sofisticación adaptativa del aparato yihadista, que se reinventa constantemente en función de los espacios disponibles, las tecnologías empleadas y las vulnerabilidades de su entorno.

La sentencia SAN 3054/2018, y su confirmación en la STS 934/2019, consolidan la validez jurídica de la figura del AEI en contextos de alto riesgo, particularmente cuando la actividad delictiva se desarrolla en escenarios digitales cerrados, cifrados y estructuralmente impermeables a métodos de investigación clásicos. Lejos de constituir una técnica prospectiva o invasiva, el trabajo del agente encubierto virtual se presenta como una herramienta quirúrgica, orientada a detectar la amenaza antes de que esta se materialice.

En base a todo lo anteriormente expuesto, esta operación ratifica la utilidad, legitimidad y necesidad del Agente Encubierto Informático como mecanismo de intervención preventiva frente al terrorismo yihadista de nueva generación. Su eficacia no se limita a la obtención de pruebas, sino que permite cortar procesos de radicalización en su fase embrionaria, proteger a potenciales víctimas captadas, y preservar el principio de seguridad colectiva dentro del marco garantista del Estado de Derecho.

XIII – CONCLUSIONES

XIII - CONCLUSIONES

PRIMERA: Las organizaciones yihadistas emplean con notable eficacia agravios históricos como el recuerdo de Al-Ándalus, transformándolo en símbolo permanente de lucha, restauración religiosa y territorial, y fuente inagotable de legitimación ideológica para justificar el terrorismo contra Occidente y particularmente contra España.

SEGUNDA: Los reclutadores yihadistas explotan la necesidad humana de identidad y reconocimiento, construyendo relatos heroicos en torno a la figura del mártir como héroe comunitario, lo que convierte la radicalización en una elección atractiva y emocionalmente significativa para jóvenes marginados o desarraigados.

TERCERA: El discurso radical encuentra terreno fértil en contextos de marginalidad social, presentando la violencia como un acto legítimo de resistencia y justicia divina frente a la opresión percibida, captando especialmente a individuos vulnerables por exclusión o victimización previa.

CUARTA: La continuidad doctrinal desde Ibn Taymiyya hasta Abu Musab al-Suri, pasando por Sayyid Qutb y al-Banna, refleja una evolución estratégica constante en la que los conceptos como la jahiliyya y el takfirismo se han convertido en piedras angulares para justificar una violencia deslocalizada y globalizada.

QUINTA: La doctrina moderna, especialmente desarrollada por Al-Suri, enfatiza una yihad descentralizada e individualizada, facilitando la emergencia de actores solitarios o células independientes que dificultan significativamente la prevención y detección temprana.

SEXTA: La coexistencia sistemática entre captación presencial y digital se revela como un método de adoctrinamiento particularmente efectivo y resistente

frente a la intervención policial, combinando el carisma personal con técnicas digitales avanzadas.

SÉPTIMA: La radicalización digital no es improvisada, sino el resultado de una ingeniería psicológica sofisticada que explota la frustración, la búsqueda de significado vital, y promueve un vínculo emocional profundo con la comunidad yihadista virtual.

OCTAVA: Las organizaciones terroristas mantienen una resiliencia tecnológica excepcional, migrando constantemente entre diversas plataformas digitales Facebook, Twitter (X), Whatsapp, Telegram, Rocket.Chat, TamTam, etc. complicando sustancialmente la vigilancia y censura preventiva.

NOVENA: La propaganda digital del yihadismo emplea técnicas transmedia avanzadas (revistas digitales como Dabiq o Rumiyah), efectos visuales cinematográficos y narrativas épicas para magnificar y glorificar la violencia, maximizando así el impacto psicológico y emocional sobre sus audiencias.

DÉCIMA: España continúa siendo objetivo prioritario en el discurso yihadista global por razones históricas, geográficas y simbólicas, consolidándose en la narrativa radical como el territorio perdido de Al-Ándalus, cuya recuperación legitima ataques continuados.

UNDÉCIMA: El retorno de combatientes extranjeros a España supone una amenaza crítica por sus capacidades operativas adquiridas en zonas de conflicto, combinado con su potencial para radicalizar nuevas generaciones mediante relatos directos de experiencias bélicas.

DUODÉCIMA España experimenta un desplazamiento progresivo hacia formas más individualizadas y descentralizadas de terrorismo, multiplicándose células pequeñas y actores aislados, incrementando considerablemente los desafíos para su prevención.

DECIMOTERCERA: La figura del AEI, amparada por el artículo 282 bis de la LECrim, ha superado reiteradamente los controles judiciales, consolidándose jurisprudencialmente como una medida legítima, ética y proporcionada para prevenir delitos graves como el terrorismo yihadista en entornos digitales cerrados.

DECIMOCUARTA: La actuación encubierta del AEI ha sido esencial en la obtención de evidencias directas sobre intenciones terroristas, permitiendo una intervención temprana decisiva antes de alcanzar la fase ejecutiva, salvando vidas y asegurando la eficacia jurídica de las pruebas recabadas.

DECIMOQUINTA: El uso de Agentes Encubiertos Informáticos permite anticiparse estratégicamente a las redes de captación y adoctrinamiento digital, identificando células en formación, reclutadores emergentes y procesos de radicalización en sus fases iniciales, contribuyendo significativamente a la seguridad preventiva.

DECIMOSEXTA: La figura del AEI debe mantenerse dentro de límites éticos y jurídicos estrictamente definidos, como el principio de no provocación, proporcionalidad, necesidad y supervisión judicial constante, garantizando así que la intervención nunca derive en vulneraciones injustificadas de derechos fundamentales.

DECIMOSÉPTIMA: La eficacia operativa del AEI depende crucialmente de una formación especializada, interdisciplinar y actualizada constantemente, incorporando conocimientos jurídicos, técnicos, lingüísticos y culturales específicos para asegurar intervenciones eficaces y legítimas frente a amenazas altamente sofisticadas y adaptativas.

IX - REFERENCIAS BIBLIOGRÁFICAS

XIV - REFERENCIAS BIBLIOGRÁFICAS

14.1. BIBLIOGRAFÍA

- ABC. (2015, marzo 11). Así son los siniestros yihadistas más activos en internet. ABC. <https://www.abc.es/espana/20150311/abci-yihadistas-internet-perfil-201503091327.html>
- ABC. (2020, enero 17). Detenido en Ceuta un joven que se radicalizó por internet y planeaba un atentado. ABC.
- Achache, J. (1992). *El marketing político: manipular o convencer*. Ediciones Pirámide
- Alamillo, L. (2016). *La cadena de custodia digital y sus garantías procesales*. Revista Española de Derecho Procesal, (101), 211–239.
- Al-Fatiha Global. (2017). *Annual Report and Financial Statements 2016*. United Kingdom: Al-Fatiha Global.
- Alemán, M. D. y Escudero, C. (2007). *Fundamentos del marketing*. ESIC Editorial.
- Alonso, L. E. (2000). *La mirada cualitativa en sociología*. Fundamentos.
- Al-Suri, A. M. (2005). *The Call for a Global Islamic Resistance*. The Global Islamic resistance. https://dn720004.ca.archive.org/0/items/uri_20210329/uri.pdf
- Amarasingam, A., Maher, S., y Winter, C. (2021). *How telegram Disruption Impacts Jihadist Platform Migration*. Centre for Research and Evidence on Security Threats. <https://crestresearch.ac.uk/resources/how-telegram-disruption-impacts-jihadist-platform-migration/>
- Armstrong, G. y Kotler, P. (2003). *Fundamentos de marketing*. Pearson Educación. https://frrq.cvg.utn.edu.ar/pluginfile.php/14584/mod_resource/content/1/Fundamentos%20del%20Marketing-Kotler.pdf
- Audiencia Nacional. Sala de lo Penal, sección 1. Sentencia SAN 3380/2013, de 02 de julio del 2013.
- Audiencia Nacional. Sala de lo Penal, sección 3. Sentencia SAN 3070/2019, de 04 de junio de 2019.

- Audiencia Nacional. Sala de lo Penal, sección 3. Sentencia SAN 3462/2018, de 25 de septiembre de 2018.
- Audiencia Nacional. Sala de lo Penal, sección 3. Sentencia SAN 5421/2018, de 27 de diciembre de 2018.
- Audiencia Nacional. Sala de Apelación, sección 64. Sentencia SAN 1447/2019, de 19 de marzo de 2019.
- Audiencia Nacional. Sala de lo Penal, sección 2. Sentencia SAN 5286/2019, de 30 de diciembre de 2019.
- Audiencia Nacional. Sala de Apelación, sección 64. Sentencia SAN 2203/2020, de 20 de marzo de 2020.
- Audiencia Provincial de Illes Balears. Sentencia 854/2021, de 9 diciembre de 2021.
- Awan, I. (2017). Cyber-extremism: Isis and the power of social media. *Social Science and Public Policy*, 54 (2), 138–149.
https://www.researchgate.net/publication/315212548_Cyber-Extremism_Isis_and_the_Power_of_Social_Media
- Ballester, D. (2021). Desradicalización en el medio penitenciario español. *Revista Española de Ciencia Política*, 55, 143–169.
- Baquero, A. (2008, mayo 12). Una red de españoles conversos al Islam ultra crece en internet. *El Periódico*.
<https://www.elperiodico.com/es/politica/20080511/red-espanoles-conversos-islam-ultra-218526>
- Berriah, M. (2023). Ibn Taymiyya's Conception of Jihad: Corpus, General Aspects, and Research Perspectives. *Teosofi, Jurnal Tasawuf Dan Pemikiran Islam*, 12 (1). <https://doi.org/10.15642/teosofi.2022.12.1.43-70>
- Bauman, Z. (2000). *Modernidad líquida*. Fondo de Cultura Económica.
<https://redmovimientos.mx/wp-content/uploads/2020/07/Modernidad-L%C3%ADquida-Bauman.pdf>
- BBC. (2015, enero 12). Who were the Charlie Hebdo attackers?. *BBC*.
<https://www.bbc.com/news/world-europe-30722038>
- Belo, A., y Sainz, R. (2007). *Marketing estratégico. Segmentación y posicionamiento*. ESIC Editorial.

- Bertran y Musitu, J. (1940). *Experiencias de los Servicios de Información del Nordeste de España (SIFNE) durante la guerra: una teoría, una técnica y una escuela sobre información general*. Espasa-Calpe S.A.
- Callimachi, R. (4 de agosto, 2018). The ISIS Files. (2019). Internal Documents of the Islamic State. *The New York Times*.
<https://www.nytimes.com/interactive/2018/04/04/world/middleeast/isis-documents-mosul-iraq.html>
- Constable, S. (19 de Agosto, 2014). *Islamic State claims killing of journalist James Foley* [Video]. Youtube. The Wall Street Journal.
<https://www.youtube.com/watch?app=desktop&v=hi1b7S9yP2o>
- Constitución Española. Boletín Oficial del Estado, núm. 311, de 29 de diciembre de 1978, pp. 29313 a 29424. [https://www.boe.es/eli/es/c/1978/12/27/\(1\)](https://www.boe.es/eli/es/c/1978/12/27/(1))
- BOE. (1979). Ley Orgánica 3/1979, de 18 de diciembre, de Estatuto de Autonomía para el País Vasco. <https://www.boe.es/eli/es/lo/1979/12/18/3>
- BOE. (1982). Ley Orgánica 13/1982, de 10 de agosto, de Reintegración y Amejoramiento del Régimen Foral de Navarra.
<https://www.boe.es/eli/es/lo/1982/08/10/13>
- BOE. (1882). Real Decreto de 14 de septiembre de 1882 por el que se aprueba la Ley de Enjuiciamiento Criminal. Gaceta de Madrid. Núm. 260, de 19 de septiembre de 1882. <https://www.boe.es/buscar/act.php?id=BOE-A-1882-6036>
- BOE. (1985). Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial. Núm. 157, de 2 de julio de 1985, <https://www.boe.es/eli/es/lo/1985/07/01/6>
- BOE. (1986). Ley Orgánica 2/1986, de 13 de marzo, de Fuerzas y Cuerpos de Seguridad. Núm. 63, de 14 de marzo de 1986.
<https://www.boe.es/eli/es/lo/1986/03/13/2>
- BOE. (1987). Real Decreto 769/1987, de 19 de junio, sobre regulación de la Policía Judicial. <https://www.boe.es/eli/es/rd/1987/06/19/769>
- BOE. (1994). Ley 10/1994, de 11 de julio, de la Policía de la Generalitat-Mossos d'Esquadra. <https://www.boe.es/eli/es-ct/l/1994/07/11/10>
- BOE. (1999). Ley Orgánica 5/1999, de 13 de enero, de modificación de la Ley de Enjuiciamiento Criminal en materia de perfeccionamiento de la acción

investigadora relacionada con el tráfico ilegal de drogas y otras actividades ilícitas graves. 14 de enero de 1999. Núm. 12

<https://www.boe.es/eli/es/lo/1999/01/13/5>

BOE. (2006). Ley Orgánica 6/2006, de 19 de julio, de reforma del Estatuto de Autonomía de Cataluña. <https://www.boe.es/eli/es/lo/2006/07/19/6>

BOE. (2010). Instrumento de ratificación del Convenio sobre la Ciberdelincuencia, hecho en Budapest, 23 de noviembre de 2001. Núm. 226, de 17 de septiembre de 2010

https://www.boe.es/diario_boe/txt.php?id=BOE-A-2010-14221

BOE. (2015). Ley Orgánica 2/2015, de 30 de marzo, de reforma del Código Penal en materia de terrorismo. Núm. 77, de 31 de marzo de 2015. <https://www.boe.es/eli/es/lo/2015/03/30/2>

BOE. (2010). Ley Orgánica 5/2010, de 22 de junio, por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal. Núm. 251, de 16 de octubre de 2010.

<https://www.boe.es/eli/es/lo/2010/06/22/5>

BOE. (2015). Ley Orgánica 13/2015, de 5 de octubre, de modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica, de 6 de octubre de 2015, Núm. 239

https://www.boe.es/diario_boe/txt.php?id=BOE-A-2015-10725

BOE. (2015). Ley 41/2015, de 5 de octubre, por la que se modifica la Ley de Enjuiciamiento Criminal para la agilización de la justicia penal y el fortalecimiento de las garantías procesales. Núm. 239, de 6 de octubre de 2015, pp. 89389–89428. <https://www.boe.es/eli/es/l/2015/10/05/41>

BOE. (2020). Decreto Legislativo 1/2020, de 22 de julio, por el que se aprueba el texto refundido de las disposiciones legales vigentes en materia de Policía del País Vasco. <https://www.boe.es/eli/es-pv/dlg/2020/07/22/1>

Bueno de Mata, F. (2012). El Agente Encubierto en Internet: mentiras virtuales para alcanzar la justicia. *Universidad da Coruña*.

<https://ruc.udc.es/rest/api/core/bitstreams/7a2dd915-b4eb-433c-b6f6-69e2d7a2986a/content>

- Cano, M. A. (2011). Reflexiones y experiencias desde las entrañas del yihadismo militante. Análisis de la autobiografía de Eric Breininger. *UNISCI Discussion Papers*, (26), 221–237.
- Carter, J.A., Maher, S., y Neumann, P. (2014). Measuring Importance and Influence in Syrian Foreign Fighter Networks. *International Centre for the Study of Radicalisation*. King's College London. <https://icsr.info/2014/04/22/icsr-report-inspires-syrian-foreign-fighters/>
- Castells, M. (2005). *La era de la información volumen I: economía, sociedad y cultura. La sociedad red*. Alianza Editorial.
- Centro Memorial de las Víctimas del Terrorismo. (2018). *Informe del Centro Memorial de las víctimas del terrorismo, núm. 4. La Yihad de Europa. Desarrollo e impacto del terrorismo yihadista en los países de la Unión Europea (1994-2017)*. https://www.memorialvt.com/wp-content/uploads/2018/03/Informe04_180212.pdf
- Charity Commission for England and Wales. (2013). *Written evidence submitted by the Charity Commission [CT 15]*. Home Affairs Committee, Counter-terrorism inquiry. UK Parliament Committees. <https://committees.parliament.uk/writtenevidence/47694/pdf/>
- Charity Commission for England and Wales. (2015). *Written evidence submitted by the Charity Commission to the Home Affairs Committee inquiry into the Government's new five year strategy into countering extremism [CEX0007]*. UK Parliament Committees. <https://committees.parliament.uk/writtenevidence/59796/html/>
- CITCO. (2025). *Informe de Transparencia 2023-2024. Retirada de contenidos Terroristas*. Ministerio del Interior. Secretaría General Técnica. https://www.lamoncloa.gob.es/serviciosdeprensa/notasprensa/interior/Documentos/2025/240725-Informe_Retirada_Contentos_Terroristas_2023_2024_CITCO.pdf
- Consejo de Europa. (2001). *Convenio sobre la Ciberdelincuencia*. <https://rm.coe.int/1680081561>

- Consejo General del Poder Judicial. (2020, 21 de diciembre). El Tribunal Supremo confirma la pena de ocho años de prisión a Yusuf Galán por difundir en redes sociales contenidos a favor de Daesh. *Consejo General del Poder Judicial*.
<https://www.poderjudicial.es/cgpj/en/Iudiciary/Supreme-Court/Pressroom/Press-Archive/El-Tribunal-Supremo-confirma-la-pena-de-ocho-anos-de-prision-a--Yusuf-Galan--por-difundir-en-redes-sociales-contenidos-a-favor-de-Daesh>
- Consejo de Ministros. (2020). *Anteproyecto de Ley de Enjuiciamiento Criminal*. Ministerio de Justicia.
<https://www.mjusticia.gob.es/es/AreaTematica/ActividadLegislativa/Documents/210126%20ANTEPROYECTO%20LECRIM%202020%20INFORMACION%20PUBLICA%20%281%29.pdf>
- Cottee, S. (2015). *The Apostates: When Muslims Leave Islam*. Oxford University Press.
- De la Corte, L. (2006). *La lógica del terrorismo*. Alianza Editorial.
- De la Mata, J. R. (2017). *La investigación penal en entornos digitales: retos y garantías*. [Video]. Canal UNED.
<https://canal.uned.es/video/5a6f55f0b1111f655c8b45a8>
- Del Cerro, J. A. (2004). El sistema de garantías constitucionales en los procesos judiciales sobre criminalidad organizada. *Estudios Jurídicos del Ministerio de Justicia*, 1378.
- Departamento de Seguridad Nacional. (2025). *Informe Anual de Seguridad Nacional 2024*. Gobierno de España.
<https://www.dsn.gob.es/sites/default/files/2025-05/IASN2024%20ACCESIBLE.pdf>
- Dershowitz, A. M. (2004). *Why Terrorism Works: Understanding the Threat, Responding to the Challenge*. Yale University Press.
- Driessen, H., Vicente, J., y García-Calvo, C. (2025). New trends in jihadism and digital propaganda. *Real Instituto Elcano*.
<https://media.realinstitutoelcano.org/wp-content/uploads/2024/10/vicente-driessen-garciacalvo-new-trends-in-jihadism.pdf>

- Chiara, P. G. (2024). Towards a right to cybersecurity in EU law? The challenges of enforcement. *Computer Law & Security Review*, 53. <https://doi.org/10.1016/j.clsr.2024.105961>
- EFE. (2015, 22 de junio). Juzgan al presunto yihadista de San Pedro que intentó viajar a Siria. *La verdad*. <https://www.laverdad.es/murcia/201506/22/juzgan-presunto-yihadista-pedro-20150622003107-v.html>
- EFE. (2015, 23 de junio). Siete meses de cárcel para el yihadista de San Pedro del Pinatar, que queda en libertad. *La Verdad*. <https://www.laverdad.es/murcia/sanpedro/201506/23/siete-meses-carcel-para-20150623012818-v.html>
- EITB. (2017, julio 26). Detenido en Balmaseda por apoyar a ISIS: Un joven de 22 años detenido por apoyar al EI. *Eitb.eus* <https://www.eitb.eus/es/noticias/sociedad/detalle/4988739/detenido-balmaseda-apoyar-isis-joven-de-22-anos-detenido-por-apoyar-ei/>
- El Confidencial. (2018, febrero 15). Así reclutaba yihadistas el mayor captador español: desde su piso en Melilla y por Facebook. *El Confidencial*.
- El Mundo. (2024, 31 de diciembre). Detenidos en Elche cuatro menores acusados de preparar un atentado yihadista. *El Mundo*. <https://www.elmundo.es/espana/2024/12/31/6773bce5fdddf927c8b45a8.html>
- El Qorchi, M. (2002). Hawala: How Does This Informal Funds Transfer System Work, and Should It Be Regulated? *IMF Finance & Development*, 39. <https://doi.org/10.5089/9781451951998.022>
- El-Said, H. (2015). *New approaches to countering terrorism: Designing and evaluating counter radicalization and de-radicalization programs*. Palgrave Macmillan UK. <https://doi.org/10.1057/9781137449979>
- Estarellas y López, J. C. (2012). El agente encubierto contra el crimen organizado. En R. Magaz Álvarez (Ed.), *Criminalidad y globalización: análisis y estrategias ante grupos y organización al margen de la ley* (335–350). Instituto Universitario General Gutierrez Mellado, UNED.
- Europa Press. (2017, julio 26). Detenido en Vizcaya un marroquí de 22 años por difundir a través de Internet la ideología del grupo terrorista Daesh. *Europa Press*. <https://www.europapress.es/nacional/noticia-detenido-vizcaya->

[marroqui-22-anos-difundir-traves-internet-ideologia-grupo-terrorista-daesh-20170726081845.html](https://www.marroqui-22-anos-difundir-traves-internet-ideologia-grupo-terrorista-daesh-20170726081845.html)

Europol. (2018). *Online jihadist propaganda: 2018 in review*. Europol Internet Referral Unit.

[https://www.europol.europa.eu/cms/sites/default/files/documents/online_jihadist_propaganda - 2018 in review 0.pdf](https://www.europol.europa.eu/cms/sites/default/files/documents/online_jihadist_propaganda_-_2018_in_review_0.pdf)

Ferluga, G. (2013, julio 02). Seis años de prisión para un informático que creaba webs para yihadistas. *El País*.

https://elpais.com/politica/2013/07/02/actualidad/1372778483_697022.html

Fernández, J.J. (2021, septiembre 30). Dáesh financia con un crowdfunding clandestino el regreso de terroristas a Europa. *El Periódico*.

<https://www.elperiodico.com/es/politica/20210930/hawala-financiacion-terrorismo-islamico-yihadismo-dinero-12129325>

Fernández, J. I. (2015, abril 23). Interior cifra en 115 a los yihadistas que han partido de España hacia Siria e Irak. Antena3 noticias.

https://www.antena3.com/noticias/espana/interior-cifra-115-cifra-yihadistas-que-han-partido-espana-siria-irak_20150423571e22886584a8abb58258e4.html

Fernando, L. (2016, 28 de septiembre). Detenidos tres presuntos yihadistas en Barcelona y Melilla que operaban en Europa a través del “terrorismo informativo”. *El Mundo*.

<https://www.elmundo.es/cataluna/2016/09/28/57eb4d21e5fdea7f288b4678.html>

Fernando, L. (2021, mayo 13). Golpe de la Guardia Civil a una red yihadista asentada en prisiones que hacía proselitismo de Daesh. *El Mundo*.

<https://www.elmundo.es/espana/2021/05/13/609cfdb7fdddf8f888b4645.html>

Fiscalía de la Audiencia Nacional. (2016). *Memoria Anual de la Fiscalía de la Audiencia Nacional*.

<https://www.fiscal.es/documents/20142/502016/Memoria+Fiscal%C3%ADa+Audiencia+Nacional+2016.pdf>

- Fiscalía General del Estado. (2017). *Memoria anual de la Fiscalía General del Estado 2017*. Capítulo II.4: Fiscalía de la Audiencia Nacional. [https://www.fiscal.es/memorias/memoria2017/FISCALIA_SITE/recursos/pdf/capitulo II/cap II 4.pdf](https://www.fiscal.es/memorias/memoria2017/FISCALIA_SITE/recursos/pdf/capitulo%20II/cap%20II%204.pdf)
- Galvis, M. J. (2021). Utilidad del estudio de los patrones de pensamiento en yihadistas españoles como mecanismo de prevención frente a la radicalización. *Revista Criminalidad*, 63(2), 83-98. <https://dialnet.unirioja.es/descarga/articulo/8454622.pdf>
- Garland, D. (2001). *The Culture of Control: Crime and Social Order in Contemporary Society*. Oxford University Press.
- Gazapo Lapayese, M.J (2018). *Daesh: terrorismo global y local a medio camino entre lo físico y lo virtual*. [Tesis doctoral, Universidad Complutense de Madrid]. <https://docta.ucm.es/bitstreams/ad929a3a-4fab-4bb3-af6f-5b2edd17f220/download>
- Gil Garre, J.M (2014). *Nuestros Jihadistas volumen I*, Instituto de Seguridad Global.
- Giner Alegría, C. A. (2020). Análisis biopsicocriminal de la radicalización terrorista. En C. Payá Santos y M. González Folgado (Coords.), *La gestión del riesgo: la inseguridad jurídica y las amenazas a la seguridad* (pp. 141–170). Tirant lo Blanch.
- Gobierno de España. (2016, 28 de septiembre). La célula yihadista desarticulada hoy en España, Bélgica y Alemania representaba una amenaza grave, concreta y continuada para la seguridad en Europa. *La Moncloa*. <https://www.lamoncloa.gob.es/serviciosdeprensa/notasprensa/mir/Paginas/2016/280916luchaterrorismo.aspx>
- Gobierno de Navarra. (2018). Ley Foral 23/2018, de 19 de noviembre, de las Policías de Navarra. <https://www.lexnavarra.navarra.es/detalle.asp?r=22054>
- Gobierno de Navarra. (2002). Decreto Foral Legislativo 213/2002, de 14 de octubre, por el que se aprueba el texto refundido de la Ley Foral de Cuerpos de Policía de Navarra. <https://www.lexnavarra.navarra.es/detalle.asp?r=22060>
- González, S. (2014, noviembre 19). Conmoción en San Pedro del Pinatar por el arresto de un yihadista que quería luchar en Siria. *La Opinión de Murcia*. <https://www.laopiniondemurcia.es/municipios/2014/11/19/prision-yihadista-detenido-san-pedro-32301993.html>

- Hamid, N. (2018, 26 de abril). The British Hacker Who Became the Islamic State's Chief Terror Cybercoach: A Profile of Junaid Hussain. *Combating Terrorism Center at West Point*. <https://ctc.westpoint.edu/british-hacker-became-islamic-states-chief-terror-cybercoach-profile-junaid-hussain/>
- Hermoso, B. (2016, abril 30). Cultura y yihadismo: los dos mundos de Molenbeek. *El País*.
https://elpais.com/cultura/2016/04/30/actualidad/1462017819_037597.html
- Hogg, M. A. (2007). Uncertainty-Identity Theory. *Advances in Experimental Social Psychology*, 39, 69-126. [https://doi.org/10.1016/S0065-2601\(06\)39002-8](https://doi.org/10.1016/S0065-2601(06)39002-8)
- Intereconomía. (2017, julio 26). El yihadista detenido en Vizcaya cobraba ayudas públicas. *Intereconomía*. <https://www.intereconomia.com/noticia/yihadista-detenido-vizcaya-cobraba-ayudas-publicas-20170726-1106/>
- Jenkins, H. (2011). Transmedia storytelling and entertainment: An annotated syllabus. *Continuum: Journal of Media & Cultural Studies*, 25(1), 69–77.
- Jordán, J. y Tarrés, S. (2007). Hizb ut-Tahrir en España. *Athena Intelligence Journal*. Vol. 2, nº 2. <https://ciaotest.cc.columbia.edu/journals/aij/v2i2/0000981.pdf>
- Jordán, J. (2010). La evolución del terrorismo yihadista global después del 11-S: Repercusiones sobre la seguridad europea y española. En Jordán, J., Pozo, P., y Guindo, M. (Coord.). *Terrorismo sin fronteras actores, escenarios y respuestas en un mundo global* (17-39). Thomson Reuters Aranzadi.
- Jordán, J. (2011). Al Qaeda central, una década después del 11-S. *Análisis Grupo de Estudios en Seguridad Internacional*, GESI 9/2011. <https://www.seguridadinternacional.es/?q=es/content/al-qaeda-central-una-d%C3%A9cada-despu%C3%A9s-del-11-s>
- Kepel, G. (2001). *La yihad. Expansión y declive del islamismo*. Península Atalaya.
- Kepel, G. (2004). *The War for Muslim Minds: Islam and the West*. Harvard University Press.
- Kepel, G. (2016). *El Terror entre nosotros. Una historia de la yihad en Francia*. PenínsulaAtalaya.
- Khosrokhavar, F. (2017). *Radicalization. Why some people choose the path of violence*. The New Press.

- Kohlmann, E. (2006). The Role of Islamic Charities in International Terrorist Recruitment and Financing. Danish Institute for International Studies. DIIS Working Paper Vol. 2006 No. 7
https://pure.diis.dk/ws/portalfiles/portal/67462/DIIS_WP_2006_7.web.pdf
- Kotler, P., y Armstrong, G. (2003). *Fundamentos de marketing*. Pearson Educación.
https://frrq.cvg.utn.edu.ar/pluginfile.php/14584/mod_resource/content/1/Fundamentos%20del%20Marketing-Kotler.pdf
- Kruglanski, A. W., Gelfand, M. J., Bélanger, J. J., Sheveland, A., Hetiarachchi, M., y Gunaratna, R. (2014). The Psychology of Radicalization and Deradicalization: How Significance Quest Impacts Violent Extremism. En *Advances in Political Psychology*, 35, S1 (69 – 93). International Society of Political Psychology
- Kruglanski, A. W., y Webber, D. (2017). The social psychological makings of a terrorist. *Current Opinion in Psychology*, 19, (131-134)
<https://doi.org/10.1016/j.copsyc.2017.03.024>
- Kruglanski, A.W., Bélanger, J.J., y Gunaratna, J. (2019). *The Three Pillars of Radicalization: Needs, Narratives, and Networks*. Oxford University Press.
<https://doi.org/10.1093/oso/9780190851125.001.0001>
- Lesaca, J. (2017). *Armas de seducción masiva. La factoría audiovisual con la que Estado Islámico ha fascinado a la generación millennial*. Península, Atalaya.
- Lister, C. (2015). *The Islamic State: A Brief Introduction*. Brookings Institution Press.
- López-Muñoz, J. (2020). *Cibercriminalidad e investigación tecnológica*. Dykinson
- Lorenzo-Dus, N., y Macdonald, S. (2018). Visual Jihad: Constructing the “Good Muslim” in Online Jihadist Magazines. *Studies in Conflict & Terrorism*, 44(5), 363–386. <https://doi.org/10.1080/1057610X.2018.1559508>
- Luna, D. (2009). El terrorismo como estrategia de marketing. *Revista de Estudios de Comunicación*, 7(1), 33–51.
- Mancebo, A.J. (2018). Los donativos por internet a oenegés islámicas con sede en el Reino Unido y la financiación del Terrorismo. *Grupo de Estudios en Seguridad Internacional*. Análisis GESI 39/2018
- MEMRI TV. (2022, septiembre 18). Al Shabaab Graduation Ceremony for Suicide Battalion. MEMRI. <https://www.memri.org/tv/somali-al-shabab->

[graduation-ceremony-suicide-battalion-spokesman-jihad-against-government](#)

MEMRI TV. (2024, febrero 08). AQAP Second Video Calls for Lone Wolf Attacks on the West. MEMRI. <https://www.memri.org/tv/aqap-second-video-inspire-magazine-calls-for-lone-wolf-attacks-west-al-aqsa-flood>

Ministerio del Interior. (2017, julio 26). Detenido en Vizcaya un joven marroquí de 22 años por difundir a través de Internet la ideología del grupo terrorista DAESH. *La Moncloa*.
<https://www.lamoncloa.gob.es/serviciosdeprensa/notasprensa/mir/Paginas/2017/260717detencionyihadismo.aspx>

Ministerio del Interior. (2020). *Plan Estratégico nacional de lucha contra la radicalización violenta*. Gobierno de España.
<https://www.interior.gob.es/opencms/pdf/servicios-al-ciudadano/plan-estrategico-nacional-de-lucha-contra-la-radicalizacion-violenta/documentacion-del-plan/estrategia-interior/PLAN-ESTRATEGICO-NACIONAL.pdf>

Ministerio del Interior. (2022). *Balance de la lucha antiterrorista 2012–2021*. Gobierno de España.

Ministerio del Interior. (2025). *Informe actualizado de detenidos por terrorismo yihadista 2004–2025*. Gobierno de España.
<https://www.interior.gob.es/opencms/pdf/prensa/balances-e-informes/Lucha-contra-el-terrorismo/Lucha-antiterrorista-contra-ETA-y-el-terrorismo-internacional-XV-Legislatura-Agosto-2023/OPERACIONES-Y-DETENIDOS-TERRORISMO-YIHADISTA-DESDE-LOS-ATENTADOS-DEL-11-MARZO-2004-17-06-2025.pdf>

Mitts, T., Phillips, G., y Wallter, B.F. (2022). Studying the Impact of ISIS Propaganda Campaigns. *The Journal of Politics*. Volume 84, Number 2.. University of Chicago Press. <https://doi.org/10.1086/716281>

Moghaddam, F. M. (2005). The Staircase to Terrorism: A Psychological Exploration. *American Psychologist Association*, 60(2), 161–169.
<https://psycnet.apa.org/doi/10.1037/0003-066X.60.2.161>

- Moghadam, A. (2006). Suicide Terrorism, Occupation, and the Globalization of Martyrdom: A Critique of Dying to Win. *Studies in Conflict & Terrorism*, 29(8), 707–729. <https://doi.org/10.1080/10576100600561907>
- Moyano, M. (2011). *Factores psicosociales contribuyentes a la radicalización islamista de jóvenes en España. Construcción de un instrumento de evaluación*. [Tesis doctoral Universidad de Granada]. DIGIBUG <https://digibug.ugr.es/bitstream/handle/10481/18403/19571008.pdf?sequence=1&isAllowed=y>
- Münkler, H. (2005). *The New Wars*. Polity Press.
- Naciones Unidas (2006). *Estrategia Global contra el Terrorismo*. Asamblea General.
- Nacos, B. L. (2002). *Mass-Mediated Terrorism: The Central Role of the Media in Terrorism and Counterterrorism*. Rowman & Littlefield.
- Nance, M., & Sampson, C. (2017). *The terrorist recognition handbook: A practitioner's manual for predicting and identifying terrorist activities*. CRC Press.
- Neumann, P. R. (2016). *Radicalized: New Jihadists and the Threat to the West*. I.B. Tauris.
- OIET. (2022). *Operaciones contra el yihadismo en España en 2022*. Observatorio Internacional de Estudios sobre Terrorismo. <https://observatorioterrorismo.com/analisis/operaciones-contra-el-yihadismo-en-espana-2022/>
- OIET. (2023). *Operaciones contra el yihadismo en España en 2023*. Observatorio Internacional de Estudios sobre Terrorismo. <https://observatorioterrorismo.com/operaciones-policiales-antiyihadistas-en-espana-2023/operaciones-contra-el-yihadismo-en-espana-en-2023/>
- OIET. (2024). *Anuario del terrorismo yihadista en España 2024*. Observatorio Internacional de Estudios sobre Terrorismo. <https://observatorioterrorismo.com/eedyckaz/2025/03/ES-ANUARIO-OIET-2024.pdf>
- OTAN (2016). *NATO Glossary of Terms and Definitions*. NATO Standardization Office.
- Pras, A., Sperotto, A., Moura, G.V.M., Drago, I., Barbosa, R., Sadre, R., Schmidt, R., y Hofstede, R. (2010). Attacks by “Anonymous” WikiLeaks proponents not

- Anonymous. CTIT Technical Report 10.41. University of Twente.
<https://research.utwente.nl/files/5095223/2010-12-CTIT-TR.pdf?>
- Quintana, Y., y Tascón, M. (2012). *Ciberactivismo. Las nuevas revoluciones de las multitudes conectadas*, Los libros de la Catarata. Madrid.
- Qurashi, F. (2018). The Prevent strategy and the UK 'war on terror': Embedding infrastructures of surveillance in Muslim communities. *Palgrave Communications, Humanities and Social Sciences Communications* 4, 17.
<https://www.nature.com/articles/s41599-017-0061-9.pdf>
- Qutb, S. (2003). *Milestones*. Kazi Publications.
- Qutb, S. (2007). *Justicia Social en el Islam*. Almuzara
- Ranstorp, M. (2004). *Mapping Terrorism Research. State of the Art, Gaps and Future direction*. Routledge.
- Reinares, F. (2014). *Matadlos. Quién estuvo detrás del 11-M y por qué se atentó en España*. Galaxia Gutenberg.
- Reinares, F. (2015). Terroristas, redes y organizaciones: facetas de la actual movilización yihadista en España. *Real Instituto El Cano*. 17/2015
- Reinares, F. (2024). Caracterización social de los yihadistas en España: continuidad de atributos básicos generales y cambio de rasgos contextuales específicos. *Real Instituto Elcano*. <https://media.realinstitutoelcano.org/wp-content/uploads/2024/02/ari30-2024-reinares-caracterizacion-social-de-los-yihadistas-en-espana-continuidad-de-atributos-basicos-generales-y-cambio-de-rasgos-contextuales-especificos.pdf>
- Reinares, F., y García-Calvo, C. (2013). *Los yihadistas en España: perfil sociodemográfico de condenados por actividades terroristas o muertos en acto de terrorismo suicida entre 1996 y 2012*. (Documento de Trabajo 11/2013). Real Instituto El Cano.
<https://media.realinstitutoelcano.org/wp-content/uploads/2021/11/dt11-2013-reinares-garciacalvo-yihadistas-espana-perfil-sociodemografico-1996-2012.pdf>
- Reinares, F. y García-Calvo, C. (2016). *Estado Islámico en España*. Real Instituto Elcano. <https://www.realinstitutoelcano.org/monografias/estado-islamico-en-espana/>

- Reinares, F. y García-Calvo, C. (2018). Marroquíes y segundas generaciones entre los yihadistas en España. ARI 61/2018. Real Instituto Elcano. <https://media.realinstitutoelcano.org/wp-content/uploads/2021/11/ari61-2018-reinares-garciacalvo-marroquies-segundas-generaciones-entre-yihadistas-espana.pdf>
- Reinares, F., y García-Calvo, C. (2022). *Atentados en Barcelona y Cambrils: (I) formación de la célula de Ripoll, radicalización de sus miembros y preparación de unos actos de terrorismo a gran escala*. Documento de trabajo 3/2022. Real Instituto Elcano. <https://media.realinstitutoelcano.org/wp-content/uploads/2022/07/dt3-2022-garcia-reinares-atentados-en-barcelona-cambrils-parte1.pdf>
- Reinares, F., y García-Calvo, C. (2022). *Atentados en Barcelona y Cambrils: (II) célula de Ripoll, enlace con el aparato de seguridad exterior de Estado Islámico y combatientes terroristas extranjeros*. Documento de trabajo 4/2022. Real Instituto Elcano. <https://media.realinstitutoelcano.org/wp-content/uploads/2022/08/dt4-2022-reinares-garciacalvo-atentados-en-barcelona-y-cambrils-parte2.pdf>
- Requeijo, A. (2024, 29 de diciembre). En la mente de 7 menores yihadistas españoles: “Estado Islámico tiene razón en todo”. *El Confidencial*. https://www.elconfidencial.com/espana/2024-12-29/mente-siete-menores-yihadistas-espanoles-estado-islamico-tiene-razon_4033442/
- Rieff, D. (2016). *Elogio del olvido: Las paradojas de la memoria histórica*. Debate.
- Rodríguez, J. A. (2014, 14 de marzo). Mustafa Maya, un islamista defensor del burka y el látigo. *El País*. https://elpais.com/politica/2014/03/14/actualidad/1394802121_081835.html
- Rodríguez, J. A. (2014, 25 de agosto). Decenas de españoles combaten en las filas del Estado Islámico en Siria. *El País*. https://elpais.com/internacional/2014/08/24/actualidad/1408903594_005453.html
- Ros, M. (2016). El espionaje en España en la Guerra Civil y la Segunda Guerra Mundial: una visión general. *Diascronic. Studi di Storia Contemporanea*, (28), 1–12. <https://doi.org/10.4000/diacronie.4751>

- RTVE. (2017, julio 26). Detenido en Bizkaia un joven acusado de difundir por Internet la ideología del Estado Islámico. RTVE. <https://www.rtve.es/noticias/20170726/detenido-bizkaia-joven-acusado-difundir-internet-ideologia-del-estado-islamico/1587161.shtml>
- Ruiz Antón, L. F. (1982). *El agente provocador en el Derecho español*. EDERSA, Editoriales de Derecho Reunidas. https://www.boe.es/biblioteca_juridica/anuarios_derecho/abrir_pdf.php?id=ANU-P-1982-10011900144
- Sageman, M. (2004). *Understanding Terror Networks*. University of Pennsylvania Press.
- Sageman, M. (2008). *Leaderless Jihad: Terror Networks in the Twenty-First Century*. University of Pennsylvania Press.
- Sampedro, V., y Resina, J. M. (2010). Opinión pública y democracia deliberativa en la sociedad de Red. *Ayer. Revista De Historia Contemporánea*, 80(4), 139–162. <https://www.revistasmarcialpons.es/revistaayer/article/view/sampedro-resina-opinion-publica-democracia-deliberativa-sociedad/2113>
- Sánchez, S. (2021). Las operaciones encubiertas en España: evolución legal y perspectivas de futuro. *REDS, Revista de Derecho, Empresa y Sociedad*, 48, 55–78. <https://dialnet.unirioja.es/descarga/articulo/9967171.pdf>
- Sánchez, V. M. (2024). La importancia de la financiación del terrorismo en relación con la actividad llevada a cabo por el yihadismo. *IEEE, Instituto Español de Estudios Estratégicos*. Documento de Opinión 100/2024. https://www.defensa.gob.es/documents/2073105/2077230/La_importancia_de_la_financiaci%C3%B3n_del_terrorismo_en_relacion_con_la_actividad_llevada_a_cabo_por_el_yihadismo_2024_DIEEEO100.pdf/a60eb805-6f48-fd71-7682-0a7e643a2f57?t=1730196992560
- Sawt al Hind. (2021, marzo). Voice of Hind – Issue 13: Ansar ul Khilafah in Hind. *Al-Tamkin Media Foundation*. <https://ia903405.us.archive.org/24/items/voh-mgz/voh13-end.pdf>
- Setmariam, M. (2005). *Llamada a la resistencia islámica global*. Documento estratégico digital recuperado de archivos de inteligencia.
- Silber, M. D., y Bhatt, A. (2007). Radicalization in the West: The Homegrown Threat. *Brennan Center for Justice*

- Silva, J. M. (2000). *La expansión del derecho penal: aspectos de la política criminal en las sociedades postindustriales*. Edisofer S.L.
- Sprinzak, E. (1991). The Process of Delegitimation: Towards a Linkage Theory of Political Terrorism. *Terrorism and Political Violence*, 3 (1), 50-68. <https://doi.org/10.1080/09546559108427092>
- Suanzes, P. R. (2015, 17 de noviembre). Abdelhamid Abaaoud, el 'cerebro' belga de los ataques de París. *El Mundo*. <https://www.elmundo.es/internacional/2015/11/17/564a0ee922601d36568b4601.html>
- Sunstein, C. R. (2001). *Echo chambers: Bush v. Gore, impeachment, and beyond*. Princeton University Press.
- Swann, W. B., Jetten, J., Gómez, A., Whitehouse, H., y Bastian, B. (2015). When group membership gets personal: A theory of identity fusion. *Psychological Review*, 122(3), 532–550. <https://doi.org/10.1037/a0028589>
- Torres, M. (2009). *La dimensión propagandística del terrorismo yihadista global*, [Tesis doctoral, Universidad de Granada]. DIGIBUG. <https://digibug.ugr.es/bitstream/handle/10481/1525/16710289.pdf?sequence=1&isAllowed=y>
- Torres, M (2009). *El eco del terror: ideología y propaganda en el terrorismo yihadista*. Plaza y Valdés editores.
- Torres, M (2014). *Al-Andalus 2.0: la ciber-yihad contra España*. Biblioteca GESI
- Torres, M. (2015). ¿Es el yihadismo una ciber-amenaza?", *Revista de Occidente*, nº 406, marzo, pp. 20-34.
- Torres, M. (2016). The Caliphate is not a Tweet Away: The Social Media Experience of Al Qaeda in the Islamic Maghreb", *Studies in Conflict & Terrorism*, Vol. 39, nº 11. (pp. 968-981) <https://doi.org/10.1080/1057610X.2016.1159430>
- Torres, M. (2018). El hacktivismo como estrategia de comunicación: de anonymous al cibercalifato. *Cuadernos de Estrategia*, 197. Ministerio de Defensa, Madrid. <https://dialnet.unirioja.es/descarga/articulo/6518649.pdf>
- Torres, M. (2020). Jihadist Propaganda as a Threat Indicator: The Case of Spain. *Terrorism and Political Violence*. 32 (2), 365 - 381 <https://doi.org/10.1080/09546553.2017.1374255>

Torres, M. (2020). Lecciones aprendidas en la prevención de la radicalización online. En F. Domínguez (Dir.). *Cómo prevenir la radicalización yihadista. Prácticas exitosas, dilemas e incertidumbres*. Cuadernos del Centro Memorial de las Víctimas del Terrorismo, 10, 41 – 46

<https://www.memorialvt.com/wp-content/uploads/2020/08/FCMVTcuadernos10.pdf>

Tribunal Constitucional. (1984). STC 114/1984, de 29 de noviembre.

Tribunal Constitucional. (1999). STC 49/1999, de 5 de abril .

Tribunal Constitucional. (2000). STC 136/2000, de 29 de mayo.

Tribunal Europeo de Derechos Humanos. (1997). Caso Van Mechelen v. Netherlands. Application nos. 21363/93, 21364/93, 21427/93 and 22056/93. Sentencia de 23 de abril de 1997.

Tribunal Supremo. (1973). STS 786/1973, de 20 de febrero.

Tribunal Supremo. (1975). STS 2873/1975, de 14 de junio.

Tribunal Supremo. (1984). STS 1570/1984, de 15 de noviembre.

Tribunal Supremo. (1995). STS 818/1995, de 14 de febrero.

Tribunal Supremo. (2000). STS 489/2020, de 16 de octubre.

Tribunal Supremo. (2000). STS 1585/2000, de 17 de octubre.

Tribunal Supremo. (2004). STS 1671/2004, de 16 de diciembre.

Tribunal Supremo. (2010). STS 1094/2010, de 30 de noviembre.

Tribunal Supremo. (2010). STS 1140/2010, de 29 de diciembre.

Tribunal Supremo. (2011). STS 832/2011, de 3 de noviembre.

Tribunal Supremo. (2013). STS 427/2013, de 10 de mayo.

Tribunal Supremo. (2013). STS 575/2013, de 28 de junio.

Tribunal Supremo. (2014). STS 1057/2014, de 5 de enero.

Tribunal Supremo. (2016). STS 1546/2016, de 6 de abril.

Tribunal Supremo. (2019). STS 167/2019, de 27 de marzo.

Tribunal Supremo. (2019). STS 750/2019, de 25 de febrero.

Tribunal Supremo. (2019). ATS 5261/2019, de 27 de noviembre.

Tribunal Supremo. (2020). STS 489/2020, de 15 de octubre.

- Tribunal Supremo. (2020). STS 3448/2020, de 20 de octubre.
- Tribunal Supremo. (2021). STS 3249/2021, de 5 de octubre.
- UNODC. (2012). *The Use of the Internet for Terrorist Purposes*. United Nations Office on Drugs and Crime.
https://www.unodc.org/documents/frontpage/Use_of_Internet_for_Terrorist_Purposes.pdf
- U.S. Department of State (2019). *Country Reports on Terrorism 2019*. Bureau of Counterterrorism.
<https://www.state.gov/wp-content/uploads/2020/06/Country-Reports-on-Terrorism-2019-2.pdf>
- Vacas, F. (2011). *El terrorismo como crimen internacional: definición, naturaleza y consecuencias jurídicas internacionales para las personas*. Tirant lo Blanch.
- Vidino, L. (2010). *The New Muslim Brotherhood in the West*. Columbia University Press
- Vidino, L. (2015). Islamism in Europe. *World Watch Research*.
<https://opendoorsanalytical.org/wp-content/uploads/2014/10/Islamism-in-Europe-2015.pdf>
- Vidino, L. (2015). Carrie Rosefsky Wickham, The Muslim Brotherhood: evolution of an Islamist movement. *Religion, State and Society*, 43(2), 199–200.
<https://doi.org/10.1080/09637494.2015.1061287>
- Vidino, L. (2015). Sharia4: From Confrontational Activism to Militancy. *Perspectives on Terrorism*, Vol. 9, No. 2 (April 2015), pp. 2-16.
<https://www.jstor.org/stable/26297356>
- Vidino, L. (2019). *Al Qaeda in Europe: The New Battleground of International Jihad*. Prometheus
- Winter, C. (2015). Documenting the Virtual “Caliphate”. *Quilliam Foundation*.
<https://www.quilliaminternational.com/shop/e-publications/documenting-the-virtual-caliphate/>
- Zafra, A. (2010). *Policía infiltrado y agente encubierto*. Tirant lo Blanch.
- Zerrouky, M. (2015, noviembre 19). Attentats du 13 novembre : la radicalisation éclair de Billy du Hood. *Le Monde*. <https://www.lemonde.fr/attaques-a->

paris/article/2015/11/19/la-radicalisation-eclair-de-billy-du-hood_4813527_4809495.html

