



GOBIERNO
DE ESPAÑA

MINISTERIO
DE ASUNTOS EXTERIORES, UNIÓN EUROPEA
Y COOPERACIÓN

Fortalecimiento de la Prevención Digital contra el Extremismo Violento en la Unión Europea

Estrategias para Combatir la
Radicalización en los Entornos
Digitales y la Desinformación



OIET

OBSERVATORIO INTERNACIONAL
DE ESTUDIOS SOBRE TERRORISMO



COVITE

Colectivo de Víctimas
del Terrorismo

MARIA CANTÓ

Fortalecimiento de la Prevención Digital contra el Extremismo Violento en la Unión Europea

Estrategias para Combatir la
Radicalización en los Entornos Digitales
y la Desinformación



GOBIERNO
DE ESPAÑA

MINISTERIO
DE ASUNTOS EXTERIORES, UNIÓN EUROPEA
Y COOPERACIÓN



de la edición de: COVITE, 2026
COVITE

Apdo. de Correos 3358
20080 San Sebastián [Guipuzkoa]
[España]



de los textos: su autor

reservados todos los derechos. ni la totalidad ni parte
de esta publicación pueden reproducirse o transmitirse
de ninguna forma o por ningún medio, sea electrónico,
mecánico, reprográfico, fotoquímico, óptico, de
grabación o cualquier otra forma de almacenamiento de
información o sistema de recuperación, sin el permiso
previo y por escrito del editor.

Texto: Maria Cantó

Coordinación: Carlos Igualada

Diseño: Romina da Silva

Introducción.....	8
Metodología.....	12
1. Objetivo general y preguntas de investigación.....	13
2. Enfoque mixto y diseño general.....	14
2.1. <i>Revisión de literatura.....</i>	15
2.2. <i>Componente cuantitativo.....</i>	16
2.3. <i>Componente cualitativo.....</i>	17
3. Indicadores y sistema de codificación para el componente cuantitativo	17
4. Criterios de selección del contenido.....	18
4.1. <i>Criterios de inclusión.....</i>	19
4.2. <i>Criterios de exclusión.....</i>	21
4.3. <i>Contenidos indirectos.....</i>	22
5. Procedimiento de recopilación y revisión.....	23
6. Procedimiento de análisis de los datos.....	24
7. Consideraciones éticas.....	25
8. Limitaciones.....	26
Revisión de literatura.....	30
1. Introducción a la revisión de literatura.....	31
1.1 <i>Ámbito geográfico y alcance del estudio.....</i>	31
1.2 <i>Ideologías analizadas comparativamente.....</i>	32
1.3 <i>Fuentes y metodología de revisión.....</i>	32
1.4 <i>Estructura de la revisión.....</i>	33
2. Síntesis breve de hallazgos principales.....	34
2.1 <i>Evolución estructural del extremismo online.....</i>	34
2.2 <i>Rejuvenecimiento y presencia de menores.....</i>	34
2.3 <i>Extremismo misógino como forma emergente.....</i>	35
2.4 <i>Innovaciones tecnológicas multiplicando capacidades</i>	35
2.5 <i>Gaming y subculturas juveniles como vectores</i>	36
3. Síntesis integradora: qué aprendemos de la literatura y por qué importa	36
3.1 <i>Convergencia ideológica en arquitecturas digitales compartidas: del contenido a la estructura.....</i>	37
3.2 <i>Hibridación ideológica: cuando las fronteras entre extremismos se disuelven</i>	39
3.3 <i>Desplazamiento hacia la radicalización onlife: disolución de fronteras online/ offline</i>	40
3.4 <i>Rejuvenecimiento del extremismo: adolescentes como protagonistas versus víctimas</i>	42

3.5 Extremismo misógino: expansión del concepto de extremismo hacia el género.....	50
3.6 Innovaciones tecnológicas: de contexto a infraestructura operativa.....	52
3.7 Gaming y subculturas juveniles: camuflaje mediante normalidad.....	54
3.8 Implicaciones para la prevención: reconceptualización fundamental.....	55
3.9 Conclusión: hacia la prevención basada en evidencia del siglo XXI.....	56
Recogida de datos para el estudio.....	58
1. Diseño del estudio.....	59
2. Plataformas monitoreadas.....	59
2.1 Contexto crítico: evolución del yihadismo digital hacia la “Yihad Blanda”	62
3. Proceso de recolección de datos.....	65
4. Sistema de categorización.....	65
5. Accesibilidad diferencial.....	66
Análisis de resultados.....	68
1. Ecosistema de plataformas digitales del extremismo contemporáneo	69
1.1 Telegram: epicentro operativo del extremismo digital	72
1.2 Instagram: red de amplificación viral y puerta de entrada	75
1.3 Reddit: intelectualización pseudoacadémica del odio	77
1.4 TikTok: captación masiva de audiencia juvenil vulnerable	79
1.5 YouTube: adoctrinamiento sistemático en formato largo.....	80
1.6 Facebook: declive relativo pero persistencia institucional	82
1.7 X (Twitter): difusión rápida y debate polarizado	83
1.8 Espacios de videojuegos: vector emergente de reclutamiento juvenil	84
2. Códigos, lenguaje y símbolos identificados.....	87
2.1 Extrema derecha: descodificando.....	87
2.2 Comunidad Incel: la codificación de la misoginia.....	92
2.3 Códigos yihadistas: sistema paralelo de comunicación encriptada.....	96
2.4 La función estratégica del lenguaje codificado.....	98
3. Convergencia e hibridación ideológica: casos documentados de “White Jihad”.....	100
3.1 Apropiación narrativa entre extrema derecha y yihadismo: estructuras compartidas bajo contenidos invertidos.....	100
3.2 Yihadismo incorporando tácticas virales de extrema derecha: modernización mediante imitación.....	101
3.3 Incels fusionando blackpill con “Gran Reemplazo”: hibridación sexual-demográfica	102

3.4 Construcción de enemigos compartidos que trascienden ideología.....	103
3.5 Dinámicas de apropiación mutua en el extremismo híbrido.....	103
3.6 Implicaciones para detección, prevención, y respuesta.....	104
3.7 Necesidad de reconceptualización desde ideología hacia patrones.....	106
4. Tácticas de captación y radicalización.....	106
5. Análisis de tendencias tecnológicas.....	132
5.1. Inteligencia Artificial Generativa y Deepfakes	132
5.2. Generación de texto y video mediante IA: la industrialización del discurso extremista	134
5.3 Bots y amplificación artificial.....	135
5.4 Targeting algorítmico: el motor sistémico de la radicalización.....	139
5.5 El ecosistema tecnológico integrado.....	140
6. Patrones peligrosos y señales de alarma.....	142
Perfiles vulnerables a la radicalización.....	156
1. Introducción: complejidad de la categorización en la Era Digital	157
2. Características comunes a perfiles vulnerables.....	158
3. Perfil de vulnerabilidad primario: varón joven adulto (18-30 años) digitalmente hiperconectado	161
4. Perfil de vulnerabilidad secundario: adolescente (12-17 años) en crisis de identidad hiperconectado.....	166
5. Diferencias fundamentales entre vulnerabilidad adolescente y adulta.....	169
6. Casos fuera de categorización: la imprevisibilidad de la vulnerabilidad.....	174
Propuestas de prevención y respuesta.....	181
1. Marco regulatorio: expansión legislativa hacia el extremismo multi-ideológico....	182
1.1 El paradigma actual y sus limitaciones.....	182
1.2 Ampliación de las categorías punibles: hacia un marco multi-ideológico.....	184
1.3 Justificación mediante evidencia internacional.....	185
1.4 Regulación de Inteligencia Artificial y contenido sintético.....	185
1.5 Salvaguardas contra censura gubernamental.....	186
2. Cooperación público-privada con plataformas tecnológicas.....	186
2.1 Modelo de responsabilidad compartida.....	186
2.2 Expansión de los sistemas de detección automatizada.....	187
2.3 Hash-Sharing y bases de datos compartidas.....	188
2.4 Iniciativas específicas para espacios gaming.....	189
3. Sector Educativo: alfabetización digital sin saturación docente	189
3.1 Integración curricular en asignaturas existentes.....	189
3.2 Detección temprana mediante protocolo para orientadores.....	190

4. Herramientas para familias.....	191
4.1 <i>Guía familiar práctica de dos páginas</i>	191
4.2 <i>Identificación de señales de alarma</i>	192
5. Profesionales de salud mental: formación especializada accesible.....	192
6. Investigadores: protección institucional.....	193
6.1 <i>Protocolos institucionales recomendados</i>	193
7. Implementación gradual y evaluación continua.....	194
7.1 <i>Priorización realista de las intervenciones</i>	194
7.2 <i>Evaluación de impacto basada en evidencia</i>	194
Conclusión: de la investigación a la acción - cooperación europea como imperativo estratégico	195
Bibliografía.....	204



INTRODUCCIÓN

El presente proyecto propone una investigación integral sobre los procesos contemporáneos de radicalización ideológica en entornos digitales, centrándose en cómo las plataformas sociales, las tecnologías emergentes y las nuevas dinámicas culturales están configurando un ecosistema especialmente propicio para la difusión de discursos extremistas. En los últimos años, la radicalización online ha dejado de limitarse a espacios marginales y se ha expandido hacia plataformas de uso cotidiano, donde se combinan narrativas emocionales, contenidos altamente visuales, estrategias de polarización y técnicas de captación dirigidas a audiencias cada vez más jóvenes. Esta evolución exige un análisis riguroso que integre tanto los cambios tecnológicos como las transformaciones sociales y culturales que operan en el ámbito digital.

Entre los fenómenos más significativos y preocupantes documentados en esta investigación destaca la hibridación ideológica: la convergencia, retroalimentación y fusión de narrativas procedentes de extremismos históricamente separados que operan ahora mediante estrategias compartidas, apropiación mutua de tácticas, y construcción de enemigos comunes que trascienden divisiones ideológicas tradicionales (Observatorio Internacional de Estudios sobre Terrorismo, 2026). Este proceso de hibridación representa uno de los desarrollos más críticos del extremismo contemporáneo y constituye línea prioritaria en el campo de investigación sobre radicalización digital a nivel europeo e internacional.

La hibridación se manifiesta mediante múltiples dinámicas: la extrema derecha europea adopta la retórica yihadista sobre la “pureza” e “invasión cultural”; el yihadismo apropiándose de la estética y tácticas de comunicación desarrolladas por supremacistas blancos; las comunidades incel fusionando determinismo biológico con narrativas de “Gran Reemplazo” demográfico; y los movimientos identitarios construyendo marcos que combinan nacionalismo étnico, antifeminismo radical, teorías conspirativas antisemitas, y rechazo violento de diversidad sexual. Este fenómeno, denominado por algunos especialistas como “white jihad” (yihad blanca) cuando describe una convergencia específica entre extrema derecha y yihadismo (Koch et al., 2023; Moreno, 2024), evidencia que las fronteras tradicionales entre ideologías extremistas se están desdibujando aceleradamente en un ecosistema digital donde la circulación transnacional de contenido, la traducción automática mediante IA, y la lógica viral de

plataformas facilitan una contaminación cruzada que sería improbable en contextos offline históricos.

El estudio se fundamenta en tres pilares metodológicos principales. Por un lado, una revisión exhaustiva de literatura reciente, que permite mapear el estado actual y comprender cómo la investigación europea e internacional ha conceptualizado fenómenos como la desinformación, la gamificación de la violencia, la manipulación algorítmica, la estética extremista, las subculturas digitales y la instrumentalización de la inteligencia artificial para la propaganda ideológica. Esta revisión constituye el marco teórico necesario para interpretar las prácticas actuales de radicalización desde un enfoque comparado y transideológico.

Por otro lado, el proyecto desarrolla un análisis empírico del ecosistema digital mediante la monitorización sistemática de plataformas abiertas y grupos públicos, la observación estructurada de contenidos y la codificación de mensajes según variables que permiten identificar patrones de narrativa, emoción, lenguaje, público objetivo y riesgo. Este proceso se complementa con entrevistas a especialistas que aportan una lectura contextual de los hallazgos, así como una visión aplicada de los desafíos que enfrenta la Unión Europea en materia de prevención digital.

El cuerpo central del estudio presentará, en primer lugar, un mapa detallado de las plataformas que concentran mayor actividad extremista -desde redes sociales consolidadas hasta servidores de mensajería y espacios emergentes vinculados al gaming-, analizando el papel que desempeñan en la difusión de ideologías mediante mecanismos de viralización, anonimato o pertenencia comunitaria. A continuación, se examinarán las principales tendencias tecnológicas que están modificando de forma sustancial las capacidades de propaganda y reclutamiento: inteligencia artificial generativa, *deep fakes*, automatización mediante bots, uso de VPN y canales cifrados, criptomonedas, entornos inmersivos, así como diseños específicos que facilitan la interacción adictiva y la circulación rápida de contenidos de odio.

El análisis también abordará las tácticas comunicativas y los códigos culturales que permiten que estas ideologías resulten atractivas para determinados sectores poblacionales. Entre ellas destacan la gamificación, los memes y el humor hostil, la estetización de la masculinidad extrema, las narrativas de victimización y redención, los discursos conspirativos y las

lógicas propias de subculturas digitales como la “manosfera”¹ o los entornos incel. La identificación de estos patrones es fundamental para comprender cómo funcionan los procesos de normalización y de radicalización incremental, especialmente entre adolescentes y adultos jóvenes.

Finalmente, a partir de toda la evidencia generada, el informe ofrecerá propuestas estratégicas para reforzar la prevención digital del extremismo violento en la Unión Europea. Estas incluirán recomendaciones para el ámbito educativo, orientaciones para profesionales que trabajan con juventud, implicaciones para la gobernanza digital y pautas prácticas para la detección temprana de señales de riesgo. El proyecto culminará con la elaboración de recomendaciones que sintetizan el conocimiento obtenido y proporcione herramientas operativas para instituciones, docentes, actores comunitarios, plataformas tecnológicas y ciudadanía.

Esta investigación aspira a ofrecer una comprensión profunda, actualizada y aplicada de las dinámicas de radicalización digital que afectan al contexto europeo, y a convertir ese conocimiento en recursos concretos que fortalezcan la resiliencia democrática y la cohesión social frente a las nuevas formas de extremismo ideológico.

1 La “manosfera” o “machoesfera” es una especie de red indefinida de comunidades que dicen atender los problemas que aquejan a los hombres -por ejemplo, citas románticas, aptitud física o paternidad-, pero a menudo promueve consejos y actitudes nocivas. Tal como destaca el informe del Secretario General de las Naciones Unidas sobre Violencia contra las mujeres y las niñas, estos grupos se unen en oposición al feminismo y presentan erróneamente a los hombres como “víctimas” del actual clima social (UN WOMEN).



METODOLOGÍA

La presente investigación adopta un enfoque metodológico mixto orientado a comprender, de forma integrada, las dinámicas de radicalización ideológica en entornos digitales, las narrativas predominantes, las tácticas empleadas por actores extremistas y la vulnerabilidad diferencial de determinados colectivos. La combinación de datos cuantitativos y cualitativos permite analizar tanto los patrones visibles de difusión como los significados, motivaciones y lógicas internas de los discursos observados.

1. Objetivo general y preguntas de investigación

El presente proyecto tiene como propósito **fortalecer la prevención digital frente a diversas formas de extremismo violento de carácter ideológico** mediante el análisis sistemático y comparado de discursos, tácticas y dinámicas de radicalización presentes en los entornos digitales europeos. Con este fin, la investigación desarrolla un estudio exhaustivo de las estrategias de desinformación, propaganda, polarización y captación empleadas por diferentes actores extremistas en plataformas abiertas y grupos públicos de mensajería.

El objetivo de esta revisión no es confirmar hipótesis preestablecidas, sino mapear tendencias, identificar patrones transversales y comprender cómo distintos tipos de extremismo se adaptan, convergen y operan en un ecosistema digital profundamente fragmentado. Para ello, se analizan comparativamente tres grandes familias ideológicas²:

- yihadismo,
- extrema derecha,
- extremismo misógino / manófera / incels

El conocimiento generado constituye la base para la elaboración de recomendaciones, dirigido a profesionales del ámbito educativo y social, organizaciones de la sociedad civil, empresas tecnológicas y ciudadanía en general. A partir de este objetivo general, la investigación se estructura en torno a las siguientes preguntas guía:

² Se documentan también casos vinculados a la extrema izquierda, aunque de forma más puntual y menos recurrente que en otras ideologías, debido a un menor volumen de interacción y actividad en comparación con otros entornos extremistas analizados.

1. ¿Qué formas de desinformación, propaganda y narrativa identitaria circulan en los ecosistemas digitales analizados durante el periodo del estudio?
2. ¿Qué perfiles vulnerables son objeto habitual de ataques o discursos hostiles y qué audiencias aparecen como destinatarias prioritarias de tácticas de captación?
3. ¿Qué formatos, plataformas y tecnologías favorecen la amplificación y viralización de contenidos extremistas?
4. ¿Qué patrones de riesgo pueden detectarse al cruzar ideología, narrativa, lenguaje emocional, tipo de interacción y nivel de difusión?
5. ¿Qué perspectivas, estrategias y recomendaciones identifican los especialistas entrevistados, y cómo pueden traducirse en pautas operativas para la prevención digital?

Este enfoque permite situar el análisis en una perspectiva amplia y orientada a la acción, garantizando que los resultados no solo describen fenómenos, sino que contribuyen a orientar políticas, prácticas educativas y estrategias institucionales para reducir el impacto y la circulación del extremismo en línea.

2. Enfoque mixto y diseño general

El estudio combina tres fuentes principales de información:

- a) la revisión de literatura exhaustiva que permite situar el estudio en el marco teórico y empírico contemporáneo sobre extremismo violento, radicalización digital, desinformación y prevención;
- b) la observación sistemática de contenido abierto en plataformas digitales, que aporta datos cuantificables y comparables;
- c) entrevistas semiestructuradas a especialistas, que permiten contextualizar los hallazgos, interpretarlos críticamente y orientar el diseño de respuestas preventivas.

2.1. Revisión de literatura

La investigación incorpora una revisión de literatura orientada a identificar tendencias recientes, enfoques emergentes y buenas prácticas relacionadas con la prevención digital del extremismo violento en Europa. Esta revisión se centra en publicaciones académicas, informes institucionales, estudios técnicos y documentos de política pública de los últimos años, un periodo caracterizado por una intensa transformación tecnológica y comunicativa que ha repercutido directamente en los ecosistemas digitales donde se desarrollan los procesos de radicalización.

Se incluyen informes institucionales (ONU, Europol, Radicalisation Awareness Network), investigaciones académicas indexadas en Scopus/ Web of Science y literatura gris relevante (think tanks, observatorios, laboratorios digitales). La selección se realizó mediante búsqueda en bases de datos con términos como “online extremism”, “gaming extremism”, “micro-communities”, “online radicalization”, “AI radicalization”, “memetic warfare” y “youth online subcultures”. Las fuentes se analizan de forma integrada, priorizando tendencias comunes, vacíos de investigación y aportes metodológicos, más que un listado exhaustivo de estudios.

El propósito de esta revisión no es validar hipótesis predefinidas, sino **mapear el estado del conocimiento**, detectar líneas de análisis relevantes y examinar cómo distintas disciplinas han abordado los retos de la radicalización en línea en un contexto de cambios acelerados. La revisión permitirá observar cómo se conceptualizan fenómenos emergentes y qué áreas requieren especial atención en el desarrollo de las recomendaciones.

Entre los ámbitos que se prevé examinar se incluyen:

- el uso de **inteligencia artificial** en la creación, personalización y amplificación de contenidos extremistas;
- la **gamificación** de procesos de captación y socialización ideológica, incluyendo dinámicas de recompensa, estética lúdica y entornos de interacción propios de comunidades jóvenes;
- la **retransmisión en directo de actos violentos** o eventos simbólicos utilizados como herramientas de propaganda;

- la evolución de los formatos virales, las estéticas digitales y los códigos culturales que facilitan la difusión de narrativas hostiles;
- las estrategias institucionales y comunitarias de **prevención, alfabetización mediática y resiliencia digital** desarrolladas en los últimos años.

Esta revisión permite mantener el momentum tecnológico, incorporando las transformaciones más recientes del entorno digital y evitando que el análisis quede anclado en modelos anteriores a la actual dinámica de plataformas, algoritmos y tecnologías emergentes. Los resultados de esta lectura crítica servirán como base conceptual para orientar el enfoque metodológico mixto, contextualizar los hallazgos empíricos y fundamentar las recomendaciones.

2.2. Componente cuantitativo

La dimensión cuantitativa se basa en un muestreo de contenidos en plataformas abiertas y en grupos públicos de mensajería. Para ello se creó un perfil de observación —hombre, español, sin atributos políticos visibles— con el fin de acceder a dichos espacios sin interferencias algorítmicas asociadas a perfiles reales del equipo de investigación. Este perfil se utiliza exclusivamente para **observación pasiva**, sin interacción.

Cada unidad de contenido se registra en una base de datos estructurada que recoge variables relativas a plataforma, formato, narrativa, ideología, target atacado, audiencia a la que se dirige, tipo de interacción, engagement, contexto geográfico, uso de tecnologías y nivel de riesgo.

Los **idiomas** son variados, incluyendo aquellos de diferentes países europeos -español, inglés, ruso, francés, italiano, etc., entre otros -, así como el árabe estándar moderno (MSA) y otros dialectos (levantino, iraquí, dariya), especialmente para el ámbito del extremismo yihadista.

Además, el análisis cualitativo incorpora una distinción fundamental para este proyecto: el foco no se sitúa en detectar “radicalización” como proceso consumado, sino en identificar **indicadores de vulnerabilidad** que pueden precederla. Estos indicadores no implican intención violenta ni conducta radical, pero sí permiten reconocer cambios significativos en la manera en

que ciertos usuarios se expresan o se relacionan con contenidos digitales. Entre estos factores se incluyen variaciones bruscas en el estilo comunicativo, un incremento repentino de interacción con cuentas que difunden discursos de injusticia, martirio o identidades legitimadas mediante violencia, así como un consumo persistente de contenidos de geopolítica religiosa o de marcos rígidos basados en “pureza”, “camino correcto” o “verdad absoluta”. También podrían considerarse señales tempranas la adopción creciente de estructuras discursivas de confrontación —como el esquema “ellos VS nosotros”— o la tendencia a buscar respuestas totalizantes ante dilemas personales o sociales. Este enfoque orientado a la vulnerabilidad permite una lectura más precisa del ecosistema digital sin patologizar a individuos ni atribuirles posiciones ideológicas cerradas.

2.3. Componente cualitativo

El componente cualitativo se nutre de entrevistas semiestructuradas con profesionales, tanto españoles como europeos, de ciberseguridad, análisis de extremismo, juventud, comunicación política, inteligencia y prevención comunitaria. Para ello, se han llevado a cabo una serie de entrevistas con miembros de la inteligencia, seguridad y educación, para nutrir este informe. Además, todas las instituciones participantes, han ayudado a desarrollar las recomendaciones, compartiendo las prácticas que ejercen desde su posición para la prevención y detección del radicalismo online.

La integración de ambos planos aporta una lectura amplia -estructural, discursiva y emocional- del fenómeno.

3. Indicadores y sistema de codificación para el componente cuantitativo

Con el fin de mantener homogeneidad analítica, se estableció un catálogo cerrado de indicadores y etiquetas que se aplica a cada registro. El sistema se organiza en doce categorías principales, presentadas en la siguiente tabla para facilitar su interpretación.

Tabla 1. Sistema de categorías para la codificación del contenido digital

Categoría	Etiquetas principales	Descripción
Audiencia (receptor)	Jóvenes adultos (mujeres y hombres), adolescentes (mujeres y hombres), niños (mujeres y hombres), hombres, mujeres, gamers (mujeres y hombres), estudiantes (mujeres y hombres)	Grupo al que se dirige el mensaje.
Contexto geográfico	Ámbito global con atención especial a España y su entorno en la Unión Europea	Ubicación implícita o explícita del caso.
Formato	Meme, vídeo corto, vídeo largo, audio/podcast, texto, hilo, foro, infografía, stream, juego online	Tipo de contenido y medio expresivo.
Ideología	Yihadista, extrema_derecha (incluye ultranacionalista y supremacista), eco-extrema, conspiracionista, antisistema, misógina, antifeminista, antivacunas	Marco ideológico explícito o implícito.
Idioma	Español, inglés, francés, alemán, árabe, etc.	Lengua del contenido.
Lenguaje emocional	Miedo, ira, odio, humor, orgullo, esperanza falsa, desprecio, venganza, ironía/sátira, violencia	Clima emocional predominante.
Narrativa dominante	Victimismo, pureza identitaria, antiélite, antiglobalista, nostalgia del pasado, héroe/mártir, salvador colectivo, odio al exogrupo, anti-medios, desconfianza científica, libertad individual	Relato principal que articula el mensaje.
Nivel de riesgo	Bajo, medio, alto	Valoración según narrativa, tono e intencionalidad.
Plataforma	YouTube, Instagram, X, Facebook, TikTok, Telegram, Reddit, Twitch, Discord, Dark Web	Espacio donde se detecta el contenido.
Táctica de captación	Normalización, memificación, apelación identitaria, humor, fake news, teoría conspirativa, canal privado, gamificación, lenguaje codificado, testimonio personal	Recursos empleados para atraer o retener.
Target (objetivo)	Mujeres, población migrante, comunidad LGTBIQ, feministas, musulmanes, judíos, profesorado, periodistas, instituciones públicas, derechas, izquierdas	Grupo que aparece en el contenido como objeto del ataque.
Tipo de interacción	Difusión, reclutamiento, adoctrinamiento, movilización, desinformación	Función del contenido en la dinámica del grupo.
Tecnología empleada	IA/deepfake, criptomonedas, VPN/anonimato, dark web, plataformas inmersivas, bots	Elementos técnicos relevantes.

4. Criterios de selección del contenido

La investigación incorpora un sistema de selección que permite gestionar de forma rigurosa el volumen elevado de datos digitales y garantizar que el análisis se focaliza exclusivamente en contenidos relevantes para la comprensión de dinámicas de radicalización. Este sistema se aplica a todas las unidades de contenido recopiladas entre el 1 de julio de 2025 y el 31

de diciembre de 2025, periodo que constituye la ventana temporal oficial del estudio. Este marco anual asegura la captación de ciclos completos de actividad digital, incluyendo picos asociados a coyunturas políticas, crisis mediáticas, fechas conmemorativas y momentos de alta polarización.

4.1. Criterios de inclusión

Para el componente cuantitativo, se incorporan al análisis únicamente aquellos contenidos que cumplen al menos tres de los cinco criterios definidos. Esta exigencia permite mantener un estándar elevado de relevancia, evitar la incorporación de materiales ambiguos y reducir el sesgo derivado de publicaciones anecdóticas.

a) Referencia explícita o simbólica a ideologías extremistas o discursos de odio

El contenido debe situarse clara o simbólicamente en el campo de la radicalización o de la hostilidad ideológica. Esto puede manifestarse mediante menciones directas, utilización de símbolos, memes, códigos discursivos u otros elementos tradicionalmente empleados por comunidades extremistas. La referencia puede adoptar formas explícitas o camuflarse mediante humor, ironía o estetización digital.

Asimismo, se incluyen contenidos que, sin mostrar signos explícitos de radicalización, evidencian indicadores tempranos de vulnerabilidad, como cambios abruptos de lenguaje, adopción de marcos binarios excluyentes o interacción repetida con discursos polarizantes.

b) Intencionalidad ideológica discernible

El mensaje debe mostrar una finalidad identificable: reforzar identidades grupales, legitimar creencias extremistas, movilizar contra un exogrupo³, deshumanizar a un colectivo, o reproducir narrativas de victimización, conspiración o amenaza. Este criterio garantiza que la muestra incluya contenidos con función ideológica, no meras opiniones aisladas.

³ Un exogrupo es un grupo social al que un individuo no pertenece ni con el que se identifica, percibido como “ajeno”, “los otros” o contrarios al propio grupo (endogrupo). Se caracteriza por la falta de apego emocional, a menudo conllevando estereotipos, prejuicios o menor valoración, siendo clave en estudios de conflicto y psicología social. (Psicología y Mente, s.f).

c) Formato orientado a la viralidad

Para ser incluido, el contenido debe presentar características asociadas a una alta capacidad de difusión: brevedad, fuerte componente visual, presencia de música emocional, edición rápida, formato meme, híper-síntesis textual o contenidos diseñados para su replicación multiplataforma. Los formatos virales son determinantes en la propagación digital de discursos extremistas, especialmente entre jóvenes.

d) Orientación hacia audiencias vulnerables

Se seleccionan contenidos que apelan directa o indirectamente a grupos con mayor susceptibilidad a la influencia digital: adolescentes, jóvenes, gamers, estudiantes o usuarios que interactúan habitualmente con discursos polarizantes. La selección de este tipo de materiales permite observar estrategias de captación dirigidas hacia públicos específicos.

e) Interacción significativa

Para garantizar la inclusión únicamente de contenidos con impacto potencial, se exige la presencia de interacción medible: número de visualizaciones, comentarios, réplicas, *retweets*, reacciones, o presencia simultánea del mismo contenido en diversas plataformas. Este criterio evita el sobredimensionamiento de publicaciones marginales y favorece un análisis centrado en materiales socialmente relevantes.

En cuanto a la revisión de literatura, se rige por un conjunto de criterios que permiten asegurar que las fuentes seleccionadas son actuales, pertinentes y coherentes con el propósito del proyecto. Como requisito fundamental, únicamente se incorporan publicaciones que permiten captar el impacto de los desarrollos tecnológicos más recientes -como la inteligencia artificial generativa, la gamificación de los discursos extremistas o la retransmisión en directo de actos violentos- y su relación con la radicalización digital. Asimismo, la revisión se limita a textos publicados en español o inglés, con el fin de garantizar accesibilidad, precisión conceptual y continuidad metodológica.

Dentro de este marco temporal y lingüístico, se incluyen únicamente aquellas fuentes cuya temática guarda una relación directa con los ejes centrales del estudio: extremismo violento en entornos digitales, propaganda, desinformación, narrativas identitarias, procesos de captación, alfabetización

mediática y enfoques de prevención o resiliencia digital. Se consideran tanto contribuciones académicas revisadas por pares como informes institucionales europeos e internacionales, documentos técnicos y estudios aplicados elaborados por centros especializados en radicalización, ciberseguridad, juventud o políticas públicas.

La inclusión requiere, además, que la fuente presente una metodología clara o, en su defecto, un análisis conceptual sólido y aplicable. Se priorizan aquellos trabajos que aportan datos empíricos, marcos interpretativos recientes o descripciones de prácticas emergentes, especialmente en relación con tecnologías novedosas (IA, automatización, deepfakes, bots), estéticas juveniles, mecánicas de gamificación o nuevos formatos de difusión extremista.

4.2. Criterios de exclusión

Del análisis principal del componente cualitativo se excluyen aquellos contenidos que, aun apareciendo en el periodo de estudio, no cumplen los estándares de relevancia o fiabilidad requeridos.

Los contenidos excluidos pertenecen a alguna de las siguientes categorías:

a) Mensajes genéricos o no ideologizados

Se excluyen publicaciones sin carga extremista o sin vínculo con narrativas de odio o polarización, aunque puedan tener componentes políticos generales.

b) Contenidos con autoría dudosa

Se descartan materiales provenientes de cuentas sin contexto identificable, perfiles aparentemente automatizados (bots), usuarios con actividad mínima o dudosa o contenido imposible de verificar.

c) Material fuera del ámbito geográfico o idiomático del estudio

El análisis se circunscribe a España y a la Unión Europea, por lo que se excluyen publicaciones vinculadas exclusivamente a otros contextos, salvo cuando contengan narrativas transferibles con impacto documentado en el ecosistema europeo.

d) Contenido duplicado

Cuando un mensaje aparece replicado múltiples veces, se analiza únicamente una instancia para evitar distorsiones cuantitativas.

e) Publicaciones sin engagement

Se excluyen materiales que no presentan interacción visible, ya que no permiten inferir impacto ni circulación social.

En cuanto a la revisión de literatura, quedan excluidas todas las publicaciones cuyo contenido resulte tangencial, excesivamente general o ajeno al fenómeno de la radicalización digital. También se descartan trabajos sin rigor verificable, textos sin respaldo académico o institucional, materiales sin metodología identificable, duplicaciones innecesarias y estudios centrados exclusivamente en contextos geográficos no pertinentes para el proyecto. Las fuentes que presenten información relevante pero incompleta —o que describan tendencias emergentes aún en consolidación— pueden considerarse como material contextual y utilizarse de manera secundaria, sin formar parte del cuerpo principal de la revisión.

Esta estrategia de selección permite construir una revisión de literatura coherente, actualizada y alineada con los desafíos tecnológicos y comunicativos contemporáneos, ofreciendo una base sólida para la interpretación de los datos y para la elaboración de las recomendaciones

4.3. Contenidos indirectos

Además de los grupos anteriores, se incorpora una categoría intermedia: los contenidos indirectos. Estos materiales no presentan una orientación extremista explícita, pero sí generan duda razonable respecto a su potencial influencia ideológica, su carga emocional polarizante o su encaje

en dinámicas discursivas extremistas. Incluyen humor hostil, banalización de estereotipos, expresiones ambiguas o mensajes susceptibles de normalizar marcos radicales.

Los contenidos indirectos se integran con la clasificación de riesgo bajo, dado que, aunque no actúan como vehículos evidentes de radicalización, contribuyen a los procesos de normalización, difusión simbólica y desplazamiento de discursos hacia posiciones extremas. Su incorporación permite capturar la dimensión más difusa y cultural de la radicalización digital.

5. Procedimiento de recopilación y revisión

La recolección de datos se ha realizado de manera semanal mediante el perfil de observación creado. Cada unidad de contenido se documenta con fecha, origen, texto o link, hashtags asociados, número de visualizaciones e interacción. Una revisión completa del sistema metodológico se llevó a cabo al final del año para ajustar categorías, corregir desviaciones y mejorar la coherencia del registro.

Como parte del proceso de búsqueda y localización de contenido, se emplea un conjunto de hashtags, expresiones clave y términos asociados a discursos extremistas, utilizados únicamente como puerta de entrada a dinámicas digitales y no como criterio de radicalización.

No se trata de búsquedas que conduzcan directamente a material extremista —ya que la mayoría de hashtags son rápidamente moderados o redirigidos—, sino de una metodología que permite adentrarse en cadenas de contenido donde pueden aparecer discursos de odio, identitarios o polarizantes.

Entre los términos explorados se encuentran: *#ConvertToIslam*, *white lives matter*, *#EuropaDespierta*, *#StopIslam*, *#IdentidadNacional*, *#StopWoke*, *#FakeNews*, *#YihadOnline*, así como conceptos como “invasión cultural”, “guerra identitaria”, “antifeminism”, “identitarism”, “antifeminismo”, “European identity”, “identitario”, “yihad”, “reclutamiento online”.

Este procedimiento refleja que las búsquedas simples rara vez generan contenido relevante; la clave es seguir la espiral algorítmica en la que estas palabras funcionan como nodos que permiten rastrear la circulación de

narrativas, entender la estética digital y observar qué contenidos surgen en su proximidad.

6. Procedimiento de análisis de los datos

Una vez recopiladas y codificadas las unidades de contenido, se desarrolla un proceso de análisis sistemático orientado a identificar patrones recurrentes, relaciones internas entre categorías y tendencias emergentes en las narrativas extremistas digitales. El análisis combina técnicas descriptivas y comparativas que permiten integrar los hallazgos cuantitativos con la interpretación cualitativa, ofreciendo una visión completa del fenómeno.

El cruce de variables constituye el núcleo del análisis. Las categorías definidas previamente —plataforma, narrativa dominante, ideología, audiencia, target, lenguaje emocional, formato, nivel de riesgo o tecnología— se relacionan entre sí para identificar dinámicas significativas. **Este enfoque permite observar, por ejemplo, qué formatos son más utilizados para dirigirse a públicos específicos, qué emociones predominan en los ataques a ciertos colectivos, o qué ideologías recurren con mayor frecuencia a mensajes breves, humorísticos o visuales.**

Entre los patrones analíticos que se han examinado se incluyen relaciones funcionales entre las distintas categorías codificadas, con el fin de identificar recurrencias, regularidades y configuraciones características en los discursos observados. El análisis no se limita a combinaciones predeterminadas, sino que explora de manera abierta cómo interactúan entre sí variables como el formato, la audiencia, la narrativa, la ideología, el lenguaje emocional, el nivel de riesgo o la tecnología empleada.

Se presta especial atención a la relación entre las características formales del contenido y los públicos a los que va dirigido, lo que permite observar si determinados formatos, estilos comunicativos o estructuras narrativas se asocian de forma constante a ciertos perfiles de audiencia. Asimismo, se analiza la vinculación entre los colectivos objeto de ataque y el tono emocional empleado, con el objetivo de identificar patrones recurrentes en la construcción del exogrupo.

Otra dimensión clave del análisis es la distribución de narrativas y marcos discursivos en función de la ideología, lo que permite detectar si existen estilos, argumentos o estructuras retóricas característicos de determinados entornos digitales o comunidades ideológicas. Del mismo modo, se examinan configuraciones asociadas al riesgo, atendiendo a combinaciones de variables que puedan señalar procesos de intensificación, polarización o escalada hostil.

Además de estas relaciones, se incorporan observaciones sobre tendencias transversales, tales como procesos de normalización, desplazamiento discursivo, replicación memética o uso sistemático de determinados recursos comunicativos. Estas tendencias se evalúan tanto en términos cualitativos (significado cultural, función social del discurso) como cuantitativos (frecuencia, distribución, recurrencia).

Este enfoque flexible no solo facilita una comprensión profunda del tipo de contenidos que circulan, sino que permite identificar regularidades útiles para la elaboración de las recomendaciones: qué discursos requieren vigilancia prioritaria, qué formatos poseen mayor capacidad de penetración cultural, qué colectivos son objeto recurrente de ataques y qué señales tempranas de radicalización pueden detectarse.

La combinación de análisis cuantitativo —centrado en frecuencias, distribución y correlaciones— e interpretación cualitativa —orientada a matices, significados y lógicas discursivas— permitirá obtener conclusiones sólidas sobre las dinámicas de radicalización en el ecosistema digital.

7. Consideraciones éticas

La investigación cuantitativa se desarrolla bajo criterios estrictos de integridad científica, respeto a los derechos digitales y protección de las personas potencialmente afectadas por la recopilación y el análisis de contenido en línea. Aunque el estudio trabaja exclusivamente con información disponible en entornos digitales abiertos o grupos públicos de acceso no restringido, se han establecido salvaguardas específicas para minimizar riesgos, garantizar la confidencialidad y preservar la dignidad de los usuarios cuyas publicaciones puedan ser analizadas.

En primer lugar, la observación se realiza mediante un perfil creado exclusivamente para fines de investigación, sin interacción con otros usuarios ni participación activa en conversaciones, con el fin de evitar cualquier forma de influencia, infiltración o alteración del ecosistema digital analizado. El estudio se limita a la observación pasiva y nunca a la intervención, lo que reduce la posibilidad de afectar dinámicas reales o de exponerse a contenidos ilícitos o privados. Se trabaja exclusivamente con datos disponibles públicamente, sin solicitar acceso restringido, sin interactuar con usuarios y sin penetrar deliberadamente en espacios cifrados.

En segundo lugar, todo el material recopilado se anonimiza en los informes de análisis y en las recomendaciones. No se reproduce información personal, identificadores directos, nombres de usuario ni enlaces a perfiles concretos. Las publicaciones se describen únicamente en términos analíticos y categoriales, preservando la privacidad de los individuos y evitando la reproducción involuntaria de discursos de odio o mensajes extremistas.

La investigación se rige por los principios de necesidad, proporcionalidad, minimización de datos, no replicación y no estigmatización, evitando cualquier práctica que pueda reforzar estereotipos, reproducir violencia simbólica o contribuir a la difusión de narrativas extremistas. Las conclusiones se formulan con cautela, evitando atribuciones generalizadoras y destacando siempre la complejidad y el carácter multifactorial de los procesos de radicalización digital.

En lo relativo al componente cualitativo basado en entrevistas semiestructuradas, el proyecto aplica un conjunto de salvaguardas éticas orientadas a garantizar la protección de las personas participantes, la integridad del proceso y la gestión responsable de la información obtenida.

8. Limitaciones

A pesar del rigor metodológico aplicado, la investigación cuantitativa presenta varias limitaciones inherentes al estudio de fenómenos digitales y fluidos, que deben tenerse en cuenta al interpretar los resultados y al elaborar recomendaciones.

Una primera limitación es la **naturaleza dinámica y cambiante del entorno digital**. Las plataformas, algoritmos, comunidades y códigos culturales evolucionan con rapidez, lo que puede afectar la estabilidad de los patrones observados. Determinadas tendencias identificadas durante el periodo analizado pueden no reproducirse en ciclos posteriores o pueden mutar hacia nuevas formas de expresión.

Una segunda limitación deriva del hecho de que el estudio se basa en **datos observables en espacios públicos o de acceso abierto**, lo que excluye dinámicas que ocurren en entornos cerrados, cifrados o privados. Por tanto, aunque el análisis permite detectar tendencias generales y contenidos representativos, no puede capturar la totalidad del ecosistema extremista ni las fases más avanzadas de interacción o radicalización individual.

También existe una limitación relacionada con la **dependencia del propio algoritmo de las plataformas**, que condiciona qué contenido se muestra prioritariamente incluso en perfiles neutrales. A pesar del uso de un perfil específicamente creado para minimizar sesgos, no es posible eliminar completamente la mediación algorítmica.

Finalmente, debe señalarse que el estudio se apoya en **procesos de codificación e interpretación** que, aun realizados de forma sistemática y con criterios cerrados, implican decisiones analíticas basadas en juicio profesional. La clasificación de narrativas, emociones o niveles de riesgo puede variar según el contexto cultural o la evolución de los códigos digitales. Por ello, los resultados deben entenderse como aproximaciones informadas y no como definiciones absolutas del fenómeno.

Estas limitaciones no disminuyen la relevancia del análisis, pero sí ayudan a contextualizar y a reforzar la necesidad de actualizar periódicamente las herramientas metodológicas incluidas en las recomendaciones.

La revisión de literatura se lleva a cabo principalmente sobre fuentes disponibles en español e inglés, que constituyen los idiomas predominantes en las bases de datos académicas y los informes institucionales relevantes. Esta elección permite acceder a una parte significativa de la producción científica e institucional reciente, pero implica también que determinadas aportaciones publicadas en otros idiomas —especialmente en francés, alemán, árabe u otras lenguas vinculadas a comunidades digitales específicas— puedan no haber

sido incluidas de forma exhaustiva. Tal restricción puede limitar parcialmente la diversidad geográfica y cultural de las perspectivas consideradas.

Asimismo, una proporción importante de la literatura emergente sobre radicalización digital, cultura memética y dinámicas de plataformas se publica en formatos no tradicionales, incluidos blogs especializados, literatura gris y documentos de trabajo que no siempre cuentan con traducciones disponibles. Aunque se han incluido fuentes de alta relevancia, el acceso limitado a textos producidos exclusivamente en idiomas distintos al español o inglés puede reducir la capacidad de capturar matices lingüísticos, culturales o contextuales que influyen en la forma en que se expresan, circulan o reinterpretan ciertos discursos extremistas en entornos digitales.

El componente cualitativo basado en entrevistas presenta también limitaciones inherentes a este tipo de metodología. En primer lugar, el número de personas entrevistadas, aunque suficiente para identificar patrones y obtener perspectivas expertas, no permite representar la totalidad de enfoques existentes en los ámbitos de ciberseguridad, extremismo, juventud o prevención. Las entrevistas reflejan interpretaciones y experiencias individuales que, si bien aportan profundidad analítica, pueden estar condicionadas por el rol profesional, el ámbito de actuación o el contexto organizacional de cada participante.

En segundo lugar, la información obtenida se ve influida por la **disponibilidad, disposición y grado de apertura** de las personas entrevistadas, así como por la posible autocensura o sesgo retrospectivo al describir casos o tendencias. Además, dado el carácter sensible del objeto de estudio, algunas personas pueden optar por no compartir ciertos detalles o matices, lo que puede limitar la exhaustividad del análisis. Aunque la investigación incorpora protocolos de anonimización y consentimiento informado para mitigar estos efectos, es importante reconocer que las entrevistas no reflejan una verdad única, sino un conjunto de perspectivas complementarias que deben interpretarse dentro de su contexto.

● Diseño general

Enfoque	Mixto (cuantitativo + cualitativo)
Objetivo	Fortalecer prevención digital contra extremismo violento

● Tres componentes metodológicos

Revisión de literatura	Fuentes: Publicaciones académicas, informes institucionales (ONU, Europol, RAN), literatura gris Ámbitos: IA en extremismo, gamificación, formatos virales, estrategias prevención
Componente cuantitativo	Método: Observación pasiva sistemática de contenido abierto (Social Listening) Perfil: Observación (hombre, español, sin atributos políticos) Idiomas: Español, inglés, ruso, francés, italiano, árabe, etc Sistema de codificación: 12 categorías
Componente cualitativo	Método: Entrevistas semiestructuradas · Participantes: Profesionales de ciberseguridad, extremismo, inteligencia, educación (España y Europa) Finalidad: Contextualizar hallazgos y orientar las recomendaciones.

● Consideraciones éticas

Observación pasiva sin interacción.
Anonimización total de los usuarios.
Sólo datos públicos.
Protección psicológica investigadora.
No replicación de discursos de odio.

● Limitaciones

Naturaleza dinámica del entorno digital.
Solo contenido público (excluye espacios cifrados).
Dependencia de algoritmos de plataformas.
Revisión limitada a español e inglés.
Número limitado de entrevistas.

● Producto final

Informe sobre el Fortalecimiento de la Prevención Digital contra el Extremismo Violento en la Unión Europea.
Recomendaciones para profesionales educativos, sociales, responsables políticos y ciudadanía general.





REVISIÓN DE LITERATURA

1. Introducción a la revisión de literatura

La presente revisión sistematiza la literatura académica e institucional publicada en los últimos años, caracterizados por transformaciones aceleradas en el ecosistema digital que han reconfigurado profundamente las dinámicas de radicalización violenta en Europa y globalmente. Durante estos años, la investigación ha documentado la expansión de nuevas tecnologías—inteligencia artificial generativa, deepfakes, livestreaming, gamificación, plataformas emergentes—que han alterado tanto los riesgos como las oportunidades en materia de prevención del extremismo violento.

1.1 *Ámbito geográfico y alcance del estudio*

Aunque la revisión incorpora literatura de alcance global, dado que el extremismo digital trasciende las fronteras nacionales mediante la circulación transnacional instantánea de contenido, el foco primario se sitúa en el contexto europeo, particularmente en las dinámicas de radicalización observables en los Estados miembros de la Unión Europea. Esta delimitación geográfica responde a tres consideraciones fundamentales: primero, Europa enfrenta desafíos específicos derivados de la diversidad cultural, el multilingüismo, la historia del terrorismo reciente (especialmente el yihadista y el de extrema derecha), y los marcos legales que balancean la libertad de expresión con la prevención del discurso de odio de manera distintiva frente a otras regiones; segundo, las instituciones europeas (Europol, el EU Knowledge Hub on Prevention of Radicalisation y el European Institute for Gender Equality) han producido un corpus sustancial de investigación aplicada específicamente relevante para el contexto europeo; tercero, el proyecto busca informar políticas públicas y prácticas preventivas implementables en España y la Unión Europea, requiriendo una evidencia contextualizada frente a generalizaciones globales potencialmente inadaptadas a las realidades institucionales, legales y culturales europeas.

Sin embargo, la literatura global, especialmente la investigación del Reino Unido post-Brexit, de Estados Unidos, Canadá, Australia y la región ASEAN, se incorpora selectivamente cuando proporciona evidencia sobre fenómenos emergentes observables también en Europa (el gaming como vector de radicalización, la IA generativa y el extremismo misógino) o cuando ofrece marcos metodológicos transferibles al contexto europeo.

1.2 Ideologías analizadas comparativamente

Lejos de abordar estas ideologías como fenómenos aislados, la revisión adopta un enfoque explícitamente transversal, mostrando cómo todas comparten lógicas digitales similares: las infraestructuras tecnológicas (Telegram, Discord, subreddits y chats cifrados), los mecanismos de captación (memes, gamificación y redpilling gradual), las estéticas juveniles (la apropiación de la cultura gaming y el humor transgresor) y las dinámicas comunitarias (la creación de jerarquías internas, la competición por el estatus y la victimización colectiva), aun cuando los contenidos doctrinales difieran radicalmente. Esta aproximación permite identificar:

- Patrones estructurales que operan independientemente de la ideología específica y que pueden informar estrategias de detección, moderación y prevención aplicables a múltiples extremismos simultáneamente, frente a respuestas fragmentadas por ideología.
- Procesos de hibridación en los que extremismos históricamente separados convergen mediante la apropiación mutua de narrativas (el white jihad: la extrema derecha adoptando el lenguaje yihadista), la construcción de enemigos compartidos (el antifeminismo unificando el yihadismo, la extrema derecha y a los incels) y la fusión de frameworks ideológicos aparentemente contradictorios.
- Innovaciones tácticas desarrolladas por una ideología y posteriormente adoptadas por otras (el yihadismo incorporando memes de extrema derecha; los neonazis replicando la estructura de la célula yihadista), evidenciando que los movimientos extremistas operan mediante una lógica de innovación competitiva donde la efectividad táctica supera la lealtad ideológica.

1.3 Fuentes y metodología de revisión

La revisión integra múltiples tipos de fuentes para capturar la diversidad de perspectivas y niveles de análisis: las investigaciones académicas revisadas por pares indexadas en bases de datos como Scopus y Web of Science proporcionan rigor metodológico y marcos teóricos; los informes institucionales de organismos europeos e internacionales (Europol TE-

SAT, el EU Knowledge Hub on Prevention of Radicalisation, UNOCT, EIGE, ICCT e ICSR) aportan análisis aplicados basados en datos operativos y en la experiencia práctica de prevención; y la literatura gris de think tanks especializados, observatorios y centros de investigación (GIFCT, el Real Instituto Elcano, RAND Europe, RSIS y el Observatorio Internacional de Estudios sobre Terrorismo) proporciona análisis de tendencias emergentes frecuentemente más actualizados que las publicaciones académicas sujetas a los retrasos de la revisión por pares.

La selección de fuentes se realizó mediante una búsqueda sistemática en bases de datos utilizando términos como *online extremism*, *gaming extremism*, *digital radicalization*, *AI radicalization*, *memetic warfare*, *youth online subcultures*, *violent misogyny* y *white jihad*, priorizando publicaciones que: (a) proporcionan evidencia empírica frente a la especulación teórica, (b) abordan fenómenos post-2020 reflejando las transformaciones tecnológicas recientes, (c) ofrecen un análisis comparativo multiideológico frente al foco exclusivo en un único extremismo y (d) discuten implicaciones para la prevención y las políticas públicas frente a la descripción pura de fenómenos.

1.4 Estructura de la revisión

La revisión se organiza en tres secciones: la Sección 1, la presente, establece el marco, el alcance y la aproximación metodológica; la Sección 2 presenta una síntesis concisa de los hallazgos principales, organizados temáticamente para una lectura rápida; y la Sección 3 desarrolla extensamente una síntesis integradora que constituye la aportación analítica central, examinando en profundidad qué aprendemos de la literatura revisada, por qué los hallazgos importan y cuáles son las implicaciones críticas para la comprensión teórica del extremismo digital y para el diseño de una prevención basada en la evidencia.

Esta revisión establece desde el inicio que el extremismo digital debe entenderse como un ecosistema híbrido, dinámico y multiforme, donde convergen ideologías diversas que se adaptan —de forma paralela y frecuentemente sincronizada— a las mismas estructuras, oportunidades y vulnerabilidades de la arquitectura digital contemporánea. Comprender esta convergencia es un prerrequisito para una prevención efectiva que responda

a la complejidad real del fenómeno, frente a simplificaciones que asumen que los extremismos operan en categorías discretas y mutuamente excluyentes.

2. Síntesis breve de hallazgos principales

La literatura revisada permite identificar cinco áreas temáticas fundamentales que estructuran el conocimiento contemporáneo sobre la radicalización digital. Esta sección presenta una síntesis concisa de los hallazgos; el análisis profundo de sus implicaciones se desarrolla extensamente en la Síntesis Integradora (Sección 3).

2.1 Evolución estructural del extremismo online

- Marco histórico-evolutivo de tres generaciones de radicalización digital (GWU, 2023): transición desde foros rudimentarios hacia redes sociales, chats cifrados, y plataformas difusas.
- Internet como facilitador/acelerador no es causa suficiente (Binder & Kenyon, 2022): opera mediante cámaras de eco, algoritmos de recomendación, y refuerzo comunitario.
- La radicalización requiere interacción humana; no ocurre mediante autoradicalización absoluta (RAND, 2013).
- Diversificación ideológica documentada: ecosistema fragmentado multi-ideológico (TE-SAT, 2025).

2.2 Rejuvenecimiento y presencia de menores

- Menores entre 12-17 años participan activamente en producción propagandística, coordinación y planificación (ICSR, 2023): 43 menores condenados por terrorismo en Inglaterra/Gales 2016-2023.
- España: menores de 18 años representan 23.4% de yihadistas condenados 2012-2023 versus 17.1% en 2001-2011 (Real Instituto Elcano, 2024).

- Durante el periodo 2012-2023, los procesos de radicalización llevados a cabo de manera exclusivamente online experimentaron un incremento drástico en España hasta alcanzar el 40.4% de los casos analizados, en comparación con el periodo 2001-2011, donde esta vía digital representaba menos del 6% (concretamente el 5.5%) de los registros documentados (García-Calvo, 2024).

2.3 Extremismo misógino como forma emergente

- Misoginia estructurada como fenómeno ideológico organizado con legitimación de violencia, construcción de adversarios, proyectos ideológicos coherentes (ICCT 2023).
- Comunidades incel presentan signos de ideología extremista violenta: discursos de odio de género, victimización identitaria, movilización colectiva.
- 75% de hombres auto-identificados como incels cumplen criterios de depresión moderada/grave.
- Ciberviolencia contra mujeres como continuo estructural que reproduce jerarquías de poder mediante ataques coordinados (EIGE 2022).

2.4 Innovaciones tecnológicas multiplicando capacidades

- IA generativa transformando producción propagandística: texto, imagen, audio, video sintético mediante modelos generativos (Wan Rosli 2024).
- Deepfakes y medios sintéticos difíciles de detectar evadiendo la moderación tradicional.
- Plataformas cifradas, entornos inmersivos (metaverso/gaming), criptomonedas facilitando coordinación transnacional discreta (TE-SAT 2025).
- Livestreaming de violencia maximizando impacto propagandístico y efecto imitativo.

2.5 Gaming y subculturas juveniles como vectores

- Videojuegos explotados estructuralmente: chats, servidores privados, modificaciones, comunidades cerradas difundiendo discursos de odio (UNOCT 2022).
- Apropiación de estética gamer, humor, lenguaje juvenil elaborando narrativas extremistas atractivas para audiencias jóvenes (EU Knowledge Hub on Prevention of Radicalisation, 2022).
- Extremismo camuflado mediante memes, ironía, skins, referencias visuales, nombres de usuario con simbología codificada (RSIS 2025).
- 90.1% de procesos de radicalización yihadista en España implicaron espacios virtuales (Real Instituto Elcano 2024).

Estos hallazgos, aunque condensados, revelan transformaciones profundas que exigen análisis riguroso de sus implicaciones para prevención, políticas públicas, y comprensión teórica del extremismo contemporáneo. La siguiente sección desarrolla extensamente dicho análisis.

3. Síntesis integradora: qué aprendemos de la literatura y por qué importa

La literatura revisada permite extraer comprensión profunda, actualizada, y operativa de la radicalización digital contemporánea que trasciende la catalogación de estudios para revelar lógicas estructurales, patrones transversales, y dinámicas emergentes que deben informar prevención basada en evidencia. Esta síntesis organiza aprendizajes en ocho dimensiones críticas, desarrollando extensamente implicaciones teóricas, metodológicas, y prácticas de cada hallazgo.

3.1 Convergencia ideológica en arquitecturas digitales compartidas: del contenido a la estructura

El hallazgo más significativo que emerge de la literatura es que distintas ideologías extremistas (yihadismo, extrema derecha, misoginia) aunque presentan contenidos doctrinales mutuamente contradictorios, operan mediante estructuras digitales compartidas que generan una convergencia funcional independiente de contenido ideológico específico. Esta convergencia no es accidental sino consecuencia de la arquitectura digital contemporánea que favorece ciertos tipos de organización, comunicación, y movilización sobre otros.

Plataformas descentralizadas como infraestructura común.

Todas las ideologías documentadas utilizan un ecosistema similar de plataformas: las redes sociales *mainstream* para la captación inicial (TikTok, Instagram y YouTube), las plataformas con moderación laxa para el adoctrinamiento (Telegram, X y subreddits específicos) y los espacios completamente cerrados para la planificación operativa (Discord privado, chats cifrados y la dark web). Esta progresión —captación → adoctrinamiento → planificación— replica la estructura de un funnel comercial adaptado a la radicalización, evidenciando que el extremismo contemporáneo ha internalizado las lógicas del marketing digital y de la economía de la atención.

Implicación crítica. Los sistemas de detección algorítmica diseñados para identificar contenido específico (la propaganda del Estado Islámico frente al supremacismo blanco) fallan cuando se enfrentan a híbridos ideológicos o cuando los extremistas migran entre plataformas manteniendo la estructura organizativa, pero alterando el contenido superficial. Una prevención efectiva requiere la transición desde una detección basada en palabras clave ideológicas hacia una detección basada en patrones estructurales: la velocidad de reclutamiento, la topología de la red (la centralidad de nodos específicos), el uso de lenguaje codificado independiente de la ideología y la presencia simultánea en múltiples plataformas con roles especializados.

Dinámicas de anonimato facilitando experimentación identitaria. La literatura documenta que el anonimato digital no solo protege la identidad, sino que también permite la exploración de identidades radicales sin consecuencias sociales inmediatas en la vida offline. Un individuo puede adoptar personajes extremistas online, experimentar con el lenguaje violento

y participar en comunidades radicales, todo mientras mantiene una identidad convencional en los contextos presenciales. Esta disociación identitaria facilita la radicalización mediante la reducción de la disonancia cognitiva: no existe contradicción entre ser un estudiante universitario moderado durante el día y un participante activo en un foro neonazi durante la noche, porque las identidades operan en dominios separados y sin superposición social.

Implicación crítica. Las intervenciones familiares o educativas que confrontan al individuo con las contradicciones entre el comportamiento online y offline pueden ser contraproducentes si no reconocen que la separación identitaria es una característica funcional, y no un defecto cognitivo. La persona radicalizada online experimenta las identidades como genuinamente separadas; forzar una integración prematura sin abordar las necesidades psicológicas que la identidad radical satisface (la pertenencia, el propósito y el reconocimiento) puede profundizar el compromiso extremista como mecanismo defensivo frente a la amenaza a una identidad que proporciona una satisfacción psicológica que la vida offline no ofrece.

Gamificación como lógica transversal. Todas las ideologías han incorporado elementos de los videojuegos: los niveles de compromiso, los logros, los rankings y la competición por el estatus dentro de la comunidad. La estructura gamificada no es ornamental, sino que cumple funciones psicológicas críticas: proporciona un sentido de progresión (la sensación de avance hacia una meta), refuerza el compromiso mediante la inversión incremental (cada nivel completado hace más costoso psicológicamente abandonar) y genera diferenciación, creando jerarquías internas que motivan el activismo para ascender. Esta incorporación de mecánicas de juego evidencia que el extremismo digital ha aprendido de la industria de los videojuegos sobre la retención de usuarios y la construcción de engagement a largo plazo.

Implicación crítica. Los programas de prevención que presentan la salida del extremismo como un proceso binario (dentro/fuera) fallan porque ignoran que el extremismo gamificado construye trayectorias de progresión donde cada etapa proporciona recompensas psicológicas específicas. La desradicalización efectiva requiere proporcionar trayectorias alternativas de progresión con una estructura similar: la pertenencia → el reconocimiento → la maestría → el liderazgo, pero orientadas hacia el activismo prosocial,

el desarrollo de habilidades socialmente valiosas o la participación en comunidades constructivas que satisfacen necesidades idénticas mediante medios opuestos.

3.2 Hibridación ideológica: cuando las fronteras entre extremismos se disuelven

La literatura reciente documenta un fenómeno crítico raramente capturado por los marcos analíticos tradicionales: los extremismos históricamente separados están fusionándose mediante la apropiación mutua de narrativas, tácticas y marcos discursivos, generando híbridos ideológicos que desafían la categorización basada en un contenido político coherente. Este proceso, denominado por algunos investigadores como white jihad cuando describe la convergencia específica entre la extrema derecha y el yihadismo, representa la evolución del extremismo hacia formas más adaptativas y resilientes.

Apropiación narrativa cross-ideológica. La extrema derecha europea ha adoptado sistemáticamente la terminología yihadista —los mártires, la pureza, la invasión, la batalla final y la resistencia sagrada— aplicándola a la lucha racial y civilizacional. Los manifiestos de atacantes recientes (Christchurch, El Paso y Buffalo) combinan referencias a las cruzadas medievales con la estructura narrativa de una declaración de yihad, evidenciando que los perpetradores estudian la propaganda yihadista como modelo retórico, independientemente del rechazo absoluto del islam como religión. Paralelamente, el yihadismo contemporáneo ha incorporado tácticas de comunicación digital desarrolladas por la alt-right: los memes, los vídeos cortos profesionales, el diseño gráfico sofisticado y las narrativas aspiracionales sobre la masculinidad.

Apropiación bidireccional revela estructura profunda compartida. Ambos movimientos construyen su identidad mediante la idea de una pureza amenazada (la racial frente a la religiosa), presentan al endogrupo como víctima de un genocidio deliberado (el Gran Reemplazo frente a la occidentalización) y glorifican la violencia como un martirio heroico. La similitud estructural facilita la transferencia del lenguaje, los símbolos y las justificaciones, porque los frameworks psicológicos subyacentes son isomórficos, independientemente del contenido superficial invertido.

Construcción de enemigos compartidos. El feminismo es odiado simultáneamente por la ideología de extrema derecha (por la destrucción de la familia tradicional), la ideología yihadista (por la corrupción moral occidental) y la ideología incel (por la supuesta opresión masculina), generando una convergencia antifeminista que permite una colaboración táctica. La comunidad LGTBIQ+ es presentada por múltiples extremismos como un símbolo de decadencia civilizacional. El globalismo funciona como un término suficientemente vago para acomodar el antisemitismo (de la extrema derecha), el antioccidentalismo (del yihadismo) y el conspiracionismo genérico (de los incels y antivacunas), permitiendo una conversación mediante un lenguaje aparentemente compartido, aunque conceptualmente se refieran a enemigos diferentes.

Implicación crítica. La categorización del extremismo en silos ideológicos discretos (el antiyihadismo frente a la anti-extrema derecha) genera vacíos institucionales donde el extremismo híbrido prospera. Un individuo radicalizado en el white jihad, que combina elementos de múltiples ideologías, no encaja perfectamente en ninguna categoría existente, evadiendo la detección y cayendo en un espacio donde ningún actor se siente responsable de intervenir.

Una prevención efectiva requiere una reconceptualización que pase de la ideología específica hacia patrones transversales: la victimización colectiva presentada como un genocidio inminente, la deshumanización de los externos al grupo, la glorificación de la violencia como resistencia, las narrativas apocalípticas y la identidad construida mediante la idea de una pureza amenazada. Estos patrones operan independientemente de la justificación ideológica superficial y pueden ser detectados, intervenidos y deslegitimados mediante estrategias unificadas.

3.3 Desplazamiento hacia la radicalización onlife: disolución de fronteras online/offline

La distinción binaria entre radicalización online versus offline ha colapsado conceptualmente. La literatura documenta consistentemente que la mayoría de procesos de radicalización ocurren en entornos híbridos “onlife” donde interacciones digitales y presenciales operan sinérgicamente

reforzándose mutuamente. Este desplazamiento no es mera cuestión semántica sino refleja una transformación fundamental en cómo la radicalización opera estructuralmente.

Lo digital como acelerador con efectos multiplicativos. La investigación realizada por la RAND Corporation (2013) estableció que ningún caso documentado involucró una radicalización exclusivamente online sin interacción humana. Sin embargo, los estudios recientes del Real Instituto Elcano (2024) muestran que la radicalización exclusivamente online aumentó hasta el 40,4 % de los casos yihadistas en España, frente a menos del 6 % en el periodo anterior.

Esta aparente contradicción se resuelve al reconocer que la interacción humana también ocurre online, mediante las comunidades digitales, las mentorías virtuales y las relaciones parasociales con figuras extremistas, cumpliendo funciones que históricamente requerían el contacto presencial, pero que ahora operan de manera efectiva mediante la mediación tecnológica.

Implicación crítica. Los programas de prevención diseñados bajo el supuesto de que la radicalización requiere el contacto presencial con reclutadores fallan porque subestiman la potencia de los vínculos digitales. La relación parasocial con un YouTuber extremista, al que un individuo sigue durante meses, consumiendo contenido diariamente y sintiendo una conexión emocional mediante los comentarios y los live chats, puede ser psicológicamente más influyente que una interacción presencial ocasional con un conocido que expresa opiniones radicales.

La prevención debe reconocer que los vínculos digitales no son sustitutos inferiores de las relaciones presenciales, sino que forman una categoría propia con características distintivas: la disponibilidad constante las 24 horas del día, la ausencia de consecuencias sociales inmediatas, la capacidad de interactuar simultáneamente con múltiples figuras y comunidades, y la permanencia del contenido, lo que permite su consumo repetido.

Espacios digitales como primarios, no secundarios. Para las generaciones que han crecido con internet omnipresente, los espacios digitales no son un complemento de la vida real, sino que constituyen el dominio primario de socialización, formación de identidad y construcción de significado. La distinción entre amigos “reales” y amigos online carece

de sentido para muchos adolescentes que pasan más tiempo interactuando digitalmente con sus pares que presencialmente, cuyos vínculos emocionales más fuertes pueden ser con personas conocidas exclusivamente online y cuyas comunidades de pertenencia existen principalmente en plataformas digitales.

Implicación crítica. Las intervenciones que desestiman la importancia de los vínculos digitales —como padres que afirman que los amigos online no son amigos reales o educadores que minimizan la relevancia de las comunidades digitales— generan una alienación adicional, porque invalidan experiencias que los jóvenes perciben como genuinas y significativas.

Una aproximación efectiva requiere reconocer la legitimidad de los vínculos digitales, al tiempo que se proporcionan herramientas para la evaluación crítica de las relaciones online, la identificación de dinámicas de manipulación y el desarrollo de un equilibrio saludable entre la socialización digital y presencial. Este enfoque debe respetar la importancia de ambos dominios, en lugar de establecer una jerarquización en la que lo presencial se considere “real” y lo digital “inauténtico”.

3.4 Rejuvenecimiento del extremismo: adolescentes como protagonistas versus víctimas

El rejuvenecimiento del extremismo violento constituye uno de los hallazgos más consistentes y preocupantes. Los datos europeos documentan que los menores de 12-17 años no solo consumen propaganda extremista, sino que participan activamente en la producción propagandística, la coordinación operativa y la planificación de ataques. Inglaterra y Gales registraron a 43 menores condenados por delitos de terrorismo entre 2016 y 2023, algunos tan jóvenes como de 13 años en el momento de los hechos.

En España, el Real Instituto Elcano (2024) documenta que los menores de 18 años representan el 23,4 % de los yihadistas condenados en el periodo 2012-2023, comparado con el 17,1 % registrado en el periodo anterior (2001-2011), evidenciando una tendencia creciente y sostenida hacia la participación juvenil en el extremismo violento. Esta preocupante realidad se consolida en las estadísticas más recientes: de acuerdo con los datos publicados en el Anuario del Terrorismo Yihadista 2025 del Observatorio

Internacional de Estudios sobre Terrorismo (OIET), el rejuvenecimiento de las redes de captación ha alcanzado cotas históricas. El balance oficial revela que casi la mitad de los detenidos por actividades vinculadas al yihadismo en España (el 48 %) corresponde a menores de 25 años, confirmando que las plataformas digitales y las nuevas dinámicas de adoctrinamiento han convertido a las cohortes más jóvenes en el objetivo prioritario del terrorismo contemporáneo (OIET, 2026).

Este fenómeno exige una reconceptualización fundamental de cómo entendemos el rol de los menores en el extremismo: desde las víctimas pasivas del reclutamiento adulto hacia agentes activos con capacidad operativa real, producción propagandística sofisticada y participación en la planificación de ataques. Sin embargo, esta reconceptualización no puede abandonar simultáneamente el reconocimiento de la vulnerabilidad específica derivada del desarrollo neurológico incompleto, de la susceptibilidad aumentada a la influencia social y de la capacidad limitada para evaluar las consecuencias a largo plazo de las decisiones tomadas durante la adolescencia. El desafío crítico es integrar ambas perspectivas —la agencia operativa y la vulnerabilidad en el desarrollo mental— en los marcos legales, las políticas preventivas y las aproximaciones de desradicalización que actualmente oscilan entre los extremos del tratamiento punitivo adulto frente a la protección infantil que minimiza la gravedad de la amenaza.

La velocidad de la radicalización adolescente y las ventanas de intervención comprimidas constituyen otro aspecto central. La literatura documenta que los adolescentes se radicalizan significativamente más rápido que los adultos: los procesos que en los adultos requieren meses o años pueden completarse en semanas cuando el sujeto es adolescente. El ICSR (2023) documenta casos en los que menores transitaban desde la exposición inicial a la propaganda hasta la planificación operativa activa en menos de seis semanas. Esta velocidad acelerada deriva de la combinación de factores estructurales y del desarrollo mental: el consumo intensivo de contenido digital (los adolescentes europeos promedian entre 6 y 8 horas diarias en plataformas digitales según los datos de 2024 de la Organización Mundial de la Salud en 2024), la capacidad de pensamiento crítico menos desarrollada para resistir la manipulación y detectar inconsistencias lógicas en las narrativas extremistas, la mayor impulsividad característica del desarrollo prefrontal incompleto que reduce la evaluación de las consecuencias a largo

plazo y la búsqueda activa de identidad y pertenencia durante un periodo vital caracterizado por la incertidumbre identitaria, que el extremismo satisface mediante narrativas que proporcionan una certeza absoluta, un propósito claro y una comunidad de pertenencia inmediata.

Adicionalmente, los adolescentes digitalmente nativos operan con fluidez en ecosistemas tecnológicos que los adultos experimentan como complejos o intimidantes. La capacidad de los jóvenes para adoptar identidades múltiples, descifrar lenguajes encriptados y transitar entre diversas plataformas digitales facilita su inmersión en las redes radicales. Este ecosistema hace que el extremismo sea percibido por el adolescente como una evolución natural de su vida digital y no como la ruptura ideológica radical que experimentan los adultos.

Implicación crítica para sistemas de prevención y respuesta.

La ventana de intervención con adolescentes es críticamente más estrecha que con los adultos. En los casos de radicalización acelerada, el margen de actuación colapsa de meses a semanas o incluso días. El sistema educativo convencional resulta inviable ante esta urgencia: la cadena de detección docente, derivación, diagnóstico e intervención activa un procesamiento burocrático que consume semanas o meses. Durante este retraso sistémico, el menor completa su radicalización ideológica y avanza hacia la planificación operativa concreta. Esta latencia institucional es del todo incompatible con la velocidad de la radicalización juvenil contemporánea.

La prevención efectiva exige protocolos de respuesta rápida. La detección de señales tempranas debe activar una intervención inmediata medida en días, no en semanas. Esto requiere un calendario estricto: evaluación inicial en 24-48 horas, intervención especializada en menos de una semana y seguimiento intensivo durante el periodo crítico. Para lograrlo, es indispensable contar con recursos dedicados —equipos especializados con disponibilidad inmediata frente a las listas de espera habituales— y vías de derivación urgentes que eviten la burocracia ordinaria. Asimismo, es vital la capacitación masiva de los docentes para diferenciar las señales específicas de radicalización de las conductas adolescentes problemáticas comunes que no requieren atención urgente.

Cada día de exposición sin intervenir a la propaganda extremista profundiza la radicalización. Esto convierte al tiempo en una variable crítica

que las estructuras actuales de protección no están capacitadas para gestionar.

Participación operativa real versus mera exposición a propaganda. La reconceptualización de menores desde víctimas hacia agentes no es una especulación teórica sino que refleja la realidad operativa documentada donde los adolescentes desempeñan roles funcionales críticos en ecosistemas extremistas. La literatura identifica cinco categorías de participación juvenil:

1. Producción propagandística profesional. Los menores con habilidades digitales nativas producen contenido visual, edición de vídeo, diseño gráfico y gestión de redes sociales que muchos adultos extremistas carecen de la capacidad técnica para crear. Un adolescente de 15 años con experiencia en edición de TikTok puede producir una propaganda más efectiva para las audiencias jóvenes que un militante adulto con una ideología profunda, pero con analfabetismo digital.
2. Traducción y adaptación cultural. Los menores multilingües o biculturales traducen propaganda y adaptan las narrativas extremistas a contextos culturales específicos, haciendo que el contenido resulte resonante para audiencias a las que la versión original no alcanzaría de manera efectiva.
3. Reclutamiento peer-to-peer. Los adolescentes reclutan a sus pares mediante vínculos de confianza preexistentes (compañeros de clase, equipos deportivos o comunidades gaming) que un reclutador adulto externo nunca podría establecer. Un mensaje extremista entregado por un amigo cercano tiene una credibilidad y una efectividad que la propaganda impersonal no logra alcanzar.
4. Coordinación logística y operativa. Los menores gestionan la infraestructura digital (servidores de Discord, canales de Telegram o grupos encriptados), coordinan actividades, archivan propaganda, mantienen listas de contactos y desempeñan roles administrativos que liberan a los adultos para la planificación estratégica.
5. Planificación y ejecución de ataques. En los casos más extremos, los menores participan activamente en la planificación de la violencia, el reconocimiento de objetivos, la adquisición de materiales y, en algunos casos documentados, en la ejecución directa de ataques o intentos de ataque.

Esta diversidad de roles evidencia que los adolescentes no son receptores pasivos de propaganda adulta, sino contribuyentes activos cuyas capacidades técnicas, culturales, y sociales específicas hacen contribuciones que adultos no pueden replicar. Los ecosistemas extremistas contemporáneos dependen funcionalmente de participación juvenil, no meramente la toleran.

Implicación crítica para marcos legales y justicia juvenil. Los sistemas de justicia juvenil europeos fueron diseñados para la delincuencia común (hurtos, vandalismo, peleas) donde el menor comete un delito impulsivo con daño localizado y limitado. La radicalización ideológica y la planificación terrorista presentan características cualitativamente diferentes: no son impulsivas sino deliberadas y sostenidas; no son localizadas sino que tienen un potencial de daño masivo; no son temporales sino que implican un compromiso ideológico profundo que persiste más allá de intervención punitiva única.

Esta incongruencia genera un dilema fundamental: ¿tratar al menor radicalizado primariamente como amenaza de seguridad que justifica medidas punitivas severas similares a adultos? ¿O tratarlo primariamente como a un menor vulnerable que justifica medidas protectoras y rehabilitativas incluso cuando ha participado en la planificación de violencia masiva?

La literatura contemporánea argumenta que esta dicotomía es falsa. Los menores radicalizados son simultáneamente amenazas de seguridad genuinas que requieren intervención para proteger a la sociedad y menores vulnerables que merecen protección de derechos del menor y maximización de las posibilidades de rehabilitación. La resolución no es elegir una perspectiva sobre otra sino desarrollar respuestas integradas que abordan ambas realidades simultáneamente.

Encarcelamiento convencional versus desenganche integrado. La evidencia documenta que el encarcelamiento de menores radicalizados en instituciones juveniles convencionales sin programas especializados de desenganche frecuentemente profundiza la radicalización mediante múltiples mecanismos: la exposición concentrada a otros menores radicalizados creando comunidades extremistas dentro de instituciones, el aislamiento social de vínculos prosociales externos que podría facilitar desvinculación ideológica, la ausencia de intervención psicológica especializada que aborde narrativas extremistas específicas versus tratamiento genérico de conducta

antisocial, y la victimización institucional percibida (el menor experimenta encarcelamiento como persecución que confirma las narrativas extremistas sobre el estado opresivo versus consecuencia apropiada de acciones) (Cherney et al., 2022; Ronco, Sbraccia y Torrente, 2019). Asimismo, diversos estudios señalan que los entornos penitenciarios pueden convertirse en espacios de socialización extremista y fortalecimiento ideológico cuando no existen mecanismos adecuados de rehabilitación y reintegración (Neumann, 2010; Clifford, 2018).

Inversamente, los programas excesivamente indulgentes que minimizan la gravedad de la planificación terrorista tratándola como “fase adolescente” temporal pueden fallar en proporcionar estructura, consecuencias, y tratamiento intensivo necesarios para un cambio comportamental profundo. Un adolescente que ha planificado un ataque terrorista no está atravesando una fase de rebeldía propia del desarrollo, sino que ha internalizado una ideología que legitima el uso de la violencia masiva. En este contexto, una aproximación que no confronte de manera rigurosa dicha ideología mediante una intervención especializada corre el riesgo de subestimar la profundidad y complejidad del problema.

La aproximación óptima identificada en la literatura combina elementos complementarios mediante un modelo integrado. Por ejemplo, el hecho de que un menor se encuentre en situación de vulnerabilidad no lo exime de la responsabilidad de sus actos. Veamos:

- **Responsabilización clara.** El menor debe entender que la planificación de violencia tiene consecuencias serias, no es minimizable como error juvenil sin importancia. Esto requiere una intervención estructurada con restricciones apropiadas.
- **Reconocimiento de vulnerabilidad.** Simultáneamente, la intervención debe reconocer que desarrollo neurológico incompleto, susceptibilidad a influencia social, y capacidad limitada de evaluar consecuencias a largo plazo son realidades que diferencian al menor del adulto, justificando una aproximación menos punitiva y más rehabilitativa.
- **Desradicalización intensiva especializada.** Los programas que abordan específicamente narrativas extremistas mediante terapia

cognitivo-conductual adaptada, exposición a contra-narrativas, mentoría por formers (ex-extremistas desradicalizados), y reconstrucción de identidad no-extremista.

- **Integración de salud mental.** La atención a vulnerabilidades psicológicas subyacentes (depresión, ansiedad, trauma, trastornos de apego) que frecuentemente precedieron a la radicalización y deben tratarse para prevenir re-radicalización.
- **Reinserción social planificada.** La preparación cuidadosa para el retorno a la comunidad incluyendo educación continuada, desarrollo de habilidades vocacionales, reconstrucción de vínculos familiares y sociales prosociales, así como seguimiento post-liberación sostenido.
- **Balance seguridad-rehabilitación.** La evaluación continua de riesgo que permite ajustar nivel de restricción basado en el progreso real versus el periodo fijo de encarcelamiento que ignora si el menor continúa radicalizado o ha experimentado cambio genuino.

Este modelo integrado reconoce que la seguridad pública y el bienestar del menor no son objetivos mutuamente excluyentes, sino complementarios: un menor exitosamente desradicalizado y reintegrado no representa una amenaza futura, beneficiando tanto a la sociedad como al individuo. Un modelo punitivo puro, que encarcela sin desenganchar ideológicamente, puede neutralizar la amenaza temporalmente, pero termina liberando eventualmente a un individuo más radicalizado que cuando ingresó, perpetuando el ciclo. Por su parte, un modelo protector puro, que minimiza la gravedad del fenómeno, puede fallar en la interrupción de la trayectoria hacia la violencia. La integración de ambos enfoques constituye, por tanto, un prerequisite para garantizar su efectividad.

Prevención primaria versus intervención secundaria tardía.

El rejuvenecimiento hacia edades cada vez más tempranas (los casos documentados de 12-13 años) plantea una pregunta crítica: ¿a qué edad comienza la prevención apropiada? Si adolescentes de 13 años están planificando ataques, la prevención que comienza en la secundaria (14-16 años) llega demasiado tarde para un subset significativo. Esto exige el desplazamiento hacia la prevención primaria en la educación primaria (8-12 años), que construye resistencia antes de la exposición, frente a la

intervención secundaria que responde después de que la radicalización ya se haya iniciado.

La prevención primaria para niños no puede consistir en una educación explícita sobre el extremismo (desarrollamentalmente inapropiada y potencialmente contraproducente al introducir conceptos que los niños no habrían encontrado), sino en el desarrollo de capacidades transversales que proporcionan inmunidad:

- **Pensamiento crítico.** Habilidades para evaluar fuentes de información, detectar manipulación, reconocer falacias lógicas, cuestionar narrativas absolutas.
- **Alfabetización emocional.** Capacidad de identificar y gestionar emociones fuertes (ira, resentimiento, victimización) que el extremismo explota como vectores de reclutamiento.
- **Pertenencia prosocial.** Conexiones fuertes con comunidades constructivas (deportes, artes, voluntariado) que satisfacen necesidades de pertenencia que el extremismo ofrece mediante medios destructivos.
- **Exposición a diversidad.** Interacción positiva con personas de diferentes orígenes culturales, religiosos, étnicos que dificulta la deshumanización de outgroups que las narrativas extremistas requieren.
- **Resiliencia ante la adversidad.** Habilidades de afrontamiento saludables ante fracaso, rechazo, exclusión que previenen externalización de culpa y búsqueda de chivos expiatorios.

Estas capacidades no previenen específicamente el extremismo, sino que construyen una fundación psicológica y social que hace al individuo menos susceptible a múltiples amenazas (el extremismo, las adicciones, las sectas y las relaciones abusivas) mediante el fortalecimiento de factores protectores generales. La inversión en una prevención primaria comprehensiva durante la niñez es más costo-efectiva que la intervención secundaria durante la adolescencia y exponencialmente más efectiva que la respuesta terciaria post-ataque.

3.5 Extremismo misógino: expansión del concepto de extremismo hacia el género

La literatura científica documenta que las comunidades incel y la manófera presentan características estructurales idénticas a los extremismos reconocidos. Estos entornos se articulan en torno a cinco ejes fundamentales: una victimización colectiva presentada como opresión sistemática; la deshumanización del outgroup mediante la categorización de las mujeres como seres subhumanos o malévolos; la legitimación de la violencia como una resistencia válida ante la injusticia; la celebración de atacantes como Elliot Rodger o Alek Minassian bajo la figura de mártires heroicos; y la construcción de un proyecto ideológico orientado a restaurar el patriarcado mediante la fuerza (Hoffman et al., 2020; Sugiura, 2021).

La intersección crítica entre salud mental y radicalización. La investigación científica documenta que el 75% de los hombres autoidentificados como incels cumplen criterios diagnósticos de depresión moderada o grave (Costello et al., 2022). Esta extraordinaria prevalencia plantea una pregunta fundamental: ¿es el extremismo misógino un problema de salud mental o de seguridad? La literatura contemporánea demuestra que responde a ambos factores simultáneamente. Por ello, se exigen respuestas integradas que aborden las vulnerabilidades psicológicas subyacentes sin minimizar la gravedad de una ideología extremista que legitima la violencia contra las mujeres.

El blackpill⁴ opera psicológicamente como una narrativa depresiva colectiva que externaliza la responsabilidad (el fracaso romántico no es culpa mía, sino un destino biológico inevitable), mientras elimina toda esperanza de mejora (si la genética determina todo, el esfuerzo personal es inútil). Esta combinación de externalización de la culpa y eliminación de la esperanza genera un estado psicológico donde la violencia puede presentarse como la única salida racional disponible: si el sufrimiento es inevitable e inmutable, la violencia contra la fuente percibida de sufrimiento (las mujeres) o la autoviolencia (el suicidio) se normalizan como respuestas comprensibles frente a respuestas patológicas.

4 Creencia nihilista extrema dentro de la comunidad incel que sostiene que el éxito romántico y sexual está completamente determinado por genética (principalmente apariencia física) de manera inmutable, convirtiendo el esfuerzo personal en inútil y frecuentemente normalizando la violencia contra mujeres o el suicidio como únicas “salidas racionales” ante esta supuesta condena biológica irreversible.

Implicación crítica. La intervención efectiva requiere la integración de la salud mental y la desradicalización, que actualmente operan en silos profesionales separados. La salud mental sin formación en extremismo trata la ideología como un mero síntoma de una depresión subyacente, fallando en desafiar las narrativas extremistas que dan forma a la cognición depresiva. La desradicalización sin atención a la salud mental ignora la depresión clínica real, que requiere tratamiento farmacológico y terapia cognitivo-conductual. La aproximación óptima integra ambos enfoques: el tratamiento de la depresión mediante la TCC y la medicación apropiada, simultáneamente con el desafío sistemático de las narrativas deterministas biológicas que externalizan la responsabilidad y eliminan la agencia personal.

Fusión con extremismo racial y de género. Se documenta una convergencia creciente entre el extremismo misógino y el identitarismo racial mediante la fusión de la victimización sexual personal con la victimización demográfica colectiva. La *Sexual Replacement Theory* argumenta que el feminismo y la diversidad racial operan sinérgicamente para destruir a los hombres blancos: el feminismo empodera a las mujeres blancas para rechazar a los hombres blancos, mientras que la inmigración proporciona hombres no blancos que las mujeres blancas prefieren debido a una masculinidad supuestamente superior o a una menor inversión en los valores occidentales. Esta fusión eleva la misoginia personal hacia una lucha civilizacional, haciendo que la violencia anti-mujer no sea solo una venganza personal, sino también una defensa de la raza blanca frente a la extinción.

Implicación crítica. La convergencia entre la misoginia y el racismo evidencia una fluidez ideológica donde los individuos radicalizados en el extremismo misógino pueden transitar fácilmente hacia un identitarismo racial completo, y viceversa, mediante puentes narrativos que presentan ambos fenómenos como aspectos de una lucha unificada. La prevención efectiva debe enfocarse en las necesidades psicológicas subyacentes (la pertenencia, el propósito y la explicación del fracaso percibido) que múltiples ideologías satisfacen mediante un contenido intercambiable, frente a la refutación detallada de un contenido específico que puede reemplazarse manteniendo intacta la estructura psicológica.

3.6 Innovaciones tecnológicas: de contexto a infraestructura operativa

Las tecnologías emergentes han transitado desde un contexto pasivo, donde el extremismo ocurre, hacia una infraestructura activa que multiplica las capacidades propagandísticas, coordinativas y operativas de los movimientos extremistas. Esta transición requiere una reconceptualización de las respuestas tecnológicas, pasando desde la moderación reactiva del contenido hacia la prevención proactiva de capacidades.

La IA generativa industrializando la producción propagandística.

Los modelos generativos de inteligencia artificial (como GPT, DALL·E, Midjourney, las herramientas de clonación de voz o el vídeo sintético) han democratizado la producción de propaganda profesional, permitiendo que un actor solitario genere un volumen de contenido que previamente habría requerido de un equipo especializado. Más crítico aún, la IA permite una personalización masiva en la que un mismo mensaje central puede adaptarse automáticamente a múltiples demografías, idiomas y niveles de radicalización, generando una capacidad de targeting extremo que resulta prácticamente imposible mediante la producción exclusivamente humana.

Implicación crítica. La moderación basada en la detección de contenido específico enfrenta una asimetría fundamental: generar contenido extremista mediante inteligencia artificial es órdenes de magnitud más rápido que detectarlo algorítmicamente. Esta carrera armamentista entre generación y detección favorece estructuralmente a la producción de contenido.

Por ello, una respuesta efectiva no puede ser exclusivamente técnica, sino que requiere componentes educativos (alfabetización en medios sintéticos), legales (marcaje obligatorio del contenido generado por IA y responsabilidad de plataformas y desarrolladores de IA) y sociales (reducción de la demanda mediante estrategias de prevención primaria que aborden las necesidades psicológicas, identitarias y comunitarias que la propaganda extremista satisface).

Deepfakes erosionando la confianza epistémica. El impacto de los deepfakes trasciende la desinformación puntual y contribuye a erosionar la confianza fundamental en la evidencia visual y auditiva. Cuando cualquier vídeo puede ser falso, toda evidencia visual se vuelve potencialmente sospechosa, generando un escepticismo generalizado que beneficia a los

extremismos mediante la relativización de la verdad —si todo puede ser falso, “mi verdad” resulta tan válida como cualquier otra— y la deslegitimación de las instituciones, ya que los medios de comunicación, los gobiernos o la ciencia pasan a percibirse como igualmente susceptibles de manipulación.

Implicación crítica. La respuesta técnica (detectores de deepfakes) es necesaria pero insuficiente porque el impacto principal no es desinformación específica sino erosión de confianza epistémica general. Una aproximación comprehensiva requiere la alfabetización en la literacidad de los medios sintéticos desde la educación temprana, el marcaje obligatorio del contenido generado por la IA (de forma similar a las advertencias presentes en las cajetillas de tabaco) y la reconstrucción de la confianza en las instituciones verificadoras mediante una transparencia radical sobre este tipo de metodologías de verificación.

Livestreaming espectacularizando violencia. La transmisión en vivo de ataques violentos, como los tiroteos de la mezquita de Christchurch y del supermercado en Buffalo representa una evolución de la violencia terrorista hacia una lógica de performance dirigida a una audiencia global en tiempo real. El livestreaming maximiza el impacto propagandístico mediante la inmediatez, la autenticidad percibida —al tratarse de contenido no editado frente al vídeo propagandístico tradicional— y la viralización facilitada por algoritmos que priorizan el contenido en directo.

La literatura académica documenta, además, un significativo efecto corycat, en el que atacantes posteriores replican el formato de retransmisión en vivo, estableciendo patrones de imitación y aprendizaje entre distintos actores extremistas.

Implicación crítica. La moderación del *livestreaming* enfrenta un dilema temporal fundamental: el contenido debe ser detectado y eliminado en cuestión de segundos —y no de minutos— para prevenir su viralización, pero la detección automatizada de violencia en tiempo real, sin generar falsos positivos masivos (como la eliminación de transmisiones legítimas de videojuegos, deportes o protestas), resulta técnicamente extremadamente compleja.

Una posible solución consistiría en implementar retrasos obligatorios de entre 15 y 30 segundos en transmisiones clasificadas como de riesgo

potencial —por ejemplo, en función del historial del usuario, palabras clave en la descripción o la localización geográfica— permitiendo una detección automatizada previa a la difusión pública. Este enfoque buscaría equilibrar la libertad de expresión con la prevención de la espectacularización de la violencia extremista.

3.7 Gaming y subculturas juveniles: camuflaje mediante normalidad

Los videojuegos y subculturas asociadas (streaming, esports, modding) representan vectores de la radicalización cualitativamente diferentes porque se perciben como normales, recreativos, y apolíticos, proporcionando camuflaje perfecto para propaganda extremista. La literatura científica documenta que el 90.1% de los procesos de radicalización yihadista en España implicaron el uso de espacios virtuales, encontrándose muchos de estos entornos directamente vinculados al ámbito del gaming (García-Calvo, 2024; Observatorio Internacional de Estudios sobre Terrorismo, 2026).

Apropiación de cultura gamer. El extremismo contemporáneo ha apropiado sistemáticamente la estética, el humor, el lenguaje y los valores de la cultura gamer, presentando las narrativas extremistas mediante marcos que las audiencias jóvenes perciben como familiares y atractivo frente al aburrido discurso político tradicional. La propaganda extremista utiliza memes de videojuegos, referencias a personajes, logros gamificados y el humor transgresor característico de los espacios gaming, haciendo que el extremismo resulte estéticamente atractivo para una generación criada en la cultura de los videojuegos.

Servidores privados Discord como infraestructura de radicalización. La estructura de servidores Discord facilita la radicalización gradual mediante canales públicos (gaming general), semi-privados (humor políticamente incorrecto presentado como bromas), y completamente privados (propaganda explícita y planificación). El usuario ingresa por interés legítimo en el juego, y gradualmente es expuesto a contenido cada vez más extremo en canales semi-privados, y finalmente invitado a canales privados donde radicalización completa ocurre.

Implicación crítica. La prevención no puede depender exclusivamente de la moderación de plataformas, porque los servidores privados son, por

diseño, invisibles para los moderadores. La aproximación efectiva requiere de la alfabetización de los usuarios jóvenes sobre cómo el gaming es explotado para la radicalización (reconociendo las señales de escalada gradual), de una supervisión parental no invasiva que mantenga una comunicación abierta sin una vigilancia autoritaria que genere alienación, y de la colaboración con las empresas de gaming para desarrollar sistemas de detección de patrones de reclutamiento (usuarios que crean múltiples servidores con una estructura progresiva de lo público a lo privado, invitaciones masivas seguidas de purgas), sin violar la privacidad de los usuarios legítimos.

3.8 Implicaciones para la prevención: reconceptualización fundamental

La literatura revisada exige una reconceptualización fundamental de la prevención, pasando desde aproximaciones fragmentadas por ideología hacia estrategias unificadas basadas en patrones transversales; desde intervenciones reactivas post-radicalización hacia una prevención primaria comprehensiva; y desde la responsabilidad exclusiva de los actores estatales hacia una colaboración multi-actor institucionalizada.

Transición desde silos ideológicos hacia patrones transversales.

La evidencia de la convergencia ideológica y de la hibridación exige que los sistemas de detección, intervención y desradicalización transiten desde una especialización por ideología (los programas antiyihadismo frente a los anti-extrema derecha operando independientemente) hacia un enfoque unificado centrado en patrones que operan transversalmente: la victimización colectiva presentada como un genocidio inminente, la deshumanización sistemática del outgroup, la glorificación de la violencia como una resistencia heroica, las narrativas apocalípticas de batalla final y la identidad construida mediante una pureza amenazada. Estos patrones son independientes de la justificación ideológica superficial y pueden abordarse mediante metodologías unificadas.

Alfabetización digital como vacuna versus tratamiento. La prevención más efectiva ocurre antes de la exposición a la propaganda extremista, requiriendo una alfabetización digital integrada curricularmente frente a intervenciones puntuales post-detección. La literatura documenta que la alfabetización efectiva requiere exposiciones repetidas durante los años formativos, y no una sesión única. El modelo óptimo integra la alfabetización

en múltiples asignaturas (lengua: análisis crítico de la propaganda; sociales: comprensión del extremismo histórico; tecnología: funcionamiento de los algoritmos, los deepfakes y la IA) mediante entre 4 y 6 sesiones anuales desde la educación primaria, construyendo una inmunidad progresiva frente a un curso intensivo único en secundaria que llega demasiado tarde para muchos estudiantes ya expuestos.

Colaboración multi-actor como necesidad versus opción.

Ningún actor individual —los gobiernos, las plataformas tecnológicas, los educadores, las familias o la salud mental— posee capacidades suficientes para una prevención efectiva. Los gobiernos proporcionan regulación y financiamiento, pero carecen de capacidad técnica; las plataformas tienen datos y herramientas técnicas, pero carecen de legitimidad democrática; los educadores tienen acceso a los jóvenes, pero carecen de formación especializada; las familias conocen mejor a los individuos, pero carecen de recursos; y los profesionales de la salud mental tratan las vulnerabilidades, pero carecen de una comprensión específica del extremismo. La prevención efectiva requiere una colaboración institucionalizada (y no ad hoc) donde cada actor contribuya con capacidades únicas mediante protocolos establecidos, financiamiento sostenido y una rendición de cuentas clara sobre las responsabilidades respectivas.

3.9 Conclusión: hacia la prevención basada en evidencia del siglo XXI

La literatura revela que el extremismo digital ha evolucionado hacia formas cualitativa y estructuralmente diferentes del extremismo offline del siglo XX. No se trata simplemente de un extremismo tradicional trasladado a internet, sino de un fenómeno emergente con características propias derivadas de la arquitectura digital: la aceleración de los procesos de radicalización, la convergencia ideológica facilitada por la circulación transnacional de contenidos, el rejuvenecimiento dramático de los perfiles radicalizados hacia la adolescencia, la hibridación ideológica que desafía las categorías tradicionales, la explotación de las tecnologías emergentes y la apropiación de las culturas juveniles digitales.

Una respuesta efectiva requiere un reconocimiento honesto de que las instituciones, los marcos legales y las aproximaciones preventivas

heredadas de la era predigital resultan insuficientes frente a la amenaza contemporánea. Esto no implica abandonar los principios fundamentales —como la protección de los derechos humanos, el debido proceso o la proporcionalidad— sino actualizar su implementación para el contexto digital. Ello incluye una regulación de las plataformas que equilibre la libertad de expresión con la prevención del daño, la incorporación de la alfabetización digital en los currículos educativos, la institucionalización de la colaboración público-privada, el desarrollo de respuestas rápidas adaptadas a la velocidad de la radicalización adolescente y la integración de la salud mental en las estrategias de desradicalización.

La evidencia demuestra que una prevención efectiva es posible, pero requiere una voluntad política sostenida, una inversión económica significativa y el reconocimiento social de que el coste de una prevención integral es una fracción mínima del coste derivado de una respuesta reactiva posterior a un ataque, medido en vidas perdidas, salud mental destruida, cohesión social erosionada y libertades civiles restringidas mediante legislaciones de emergencia promulgadas tras atentados que podrían haberse evitado con mecanismos preventivos adecuados.

La cuestión no es si Europa puede permitirse invertir en una prevención integral, sino si puede permitirse continuar con el enfoque fragmentado actual, que deja vacíos críticos donde la radicalización florece. La literatura proporciona una hoja de ruta basada en la evidencia; su implementación depende de decisiones políticas, institucionales y sociales que deben adoptarse con urgencia, reconociendo que cada año de demora permite que una nueva generación de jóvenes europeos quede expuesta a la propaganda extremista sin las protecciones adecuadas.



RECOGIDA DE DATOS PARA EL ESTUDIO

1. Diseño del estudio

El presente análisis se enmarca en un estudio longitudinal de monitorización de contenido extremista online en el espacio europeo, con especial énfasis en España. La investigación adopta un enfoque mixto que combina metodología cuantitativa (análisis estadístico de frecuencias, distribuciones y correlaciones) con metodología cualitativa (análisis de discurso, identificación de narrativas y estudio de casos). Esta triangulación metodológica permite obtener una comprensión integral del fenómeno de la radicalización digital en sus múltiples dimensiones: estructural, discursiva, tecnológica y operativa.

El diseño del estudio se basa en la observación no participante de espacios digitales públicos y semipúblicos, respetando en todo momento los principios éticos de investigación y las normativas de protección de datos (GDPR). No se ha procedido a la identificación de individuos específicos, centrándose el análisis en patrones colectivos, narrativas compartidas y dinámicas de grupo.

2. Plataformas monitoreadas

La selección de las plataformas respondió a criterios múltiples: la prevalencia documentada en la literatura científica sobre el extremismo digital, el volumen estimado de contenido extremista basado en estudios previos, la accesibilidad técnica mediante métodos OSINT y la relevancia en el contexto europeo e iberoamericano. Se priorizaron aquellos espacios donde las investigaciones anteriores han identificado una mayor concentración de contenido extremista y una mayor capacidad de radicalización de usuarios.

El monitoreo abarcó ocho categorías de plataformas digitales:

Telegram fue identificado como una plataforma prioritaria debido a su adopción masiva por parte de las comunidades extremistas expulsadas de espacios con mayores niveles de moderación. El proceso de monitoreo implicó búsquedas sistemáticas de palabras clave en español, inglés, italiano, francés y alemán ("yihad", "identitarios", "tradición", "remigración", "incel", "antifa", "resistencia", "chad" y "reemplazo"), la identificación de canales públicos mediante enlaces compartidos en otras plataformas y el seguimiento de

las menciones cruzadas entre canales. Se crearon cuentas de investigación específicas, sin vinculación a la identidad personal, utilizando números virtuales de verificación para evitar la exposición de los datos personales de los investigadores. El monitoreo se centró en los canales públicos y los grupos semipúblicos accesibles mediante enlaces de invitación distribuidos abiertamente, excluyendo deliberadamente los intentos de acceso a grupos privados con procesos estrictos de *vetting*, por consideraciones éticas y de seguridad.

Instagram requirió una metodología diferente debido a su estructura basada en perfiles individuales, en lugar de canales. El proceso incluyó búsquedas mediante hashtags relevantes (#remigración, #Tawhid, #violencia, #reconquista, #patriotas, #yihad, #identitarios, #stopinmigración, #defendeeuropa, #Nasheed, #chad, #turecel y #blackpill), el análisis de las cuentas sugeridas por el algoritmo de Instagram tras interactuar con el contenido inicialmente identificado y el mapeo de redes mediante el seguimiento de las cuentas que múltiples perfiles extremistas seguían o mencionaban. Asimismo, se documentaron patrones de coordinación mediante el análisis del timing de las publicaciones, de los contenidos compartidos y de las frases idénticas replicadas en múltiples cuentas. La recolección se limitó exclusivamente al contenido público accesible sin necesidad de seguir cuentas privadas.

Reddit permitió el monitoreo mediante la lectura de subreddits públicos sin necesidad de participación activa. El proceso incluyó la identificación de subreddits relevantes mediante búsquedas directas y análisis de menciones cruzadas en otros espacios, la lectura sistemática de threads con un elevado número de comentarios —indicativos de discusiones activas— y la documentación de narrativas recurrentes, terminología específica y dinámicas de refuerzo grupal. Para ello, se utilizó una cuenta de investigación con historial mínimo, evitando así sesgos algorítmicos derivados de interacciones previas.

TikTok presentó desafíos específicos debido a la naturaleza altamente personalizada de su algoritmo. El monitoreo requirió la creación de una cuenta nueva sin historial previo, búsquedas iniciales mediante hashtags identificados en otras plataformas y el análisis del contenido progresivamente más extremo que el algoritmo comenzaba a recomendar tras las primeras

interacciones. Este proceso permitió documentar el denominado rabbit hole algorítmico: la manera en que la exposición inicial a contenido moderadamente transgresor conduce automáticamente a recomendaciones de contenido progresivamente más extremo. La recolección se centró en vídeos virales con un elevado número de visualizaciones y en contenidos posteriormente republicados (cross-posted) en Instagram.

YouTube fue monitoreado mediante búsquedas de términos clave, el análisis de canales enlazados desde Telegram e Instagram y la documentación de series de vídeos temáticos relacionados con ideologías extremistas. Se prestó especial atención al fenómeno de las recomendaciones algorítmicas, analizando qué contenidos sugería automáticamente la plataforma tras la visualización inicial de un vídeo identificado. El monitoreo incluyó también el análisis de los comentarios como espacios de construcción comunitaria y refuerzo ideológico.

Facebook requirió búsquedas de páginas públicas mediante términos relevantes, la identificación de grupos públicos —aquellos cuyo contenido puede visualizarse sin necesidad de adhesión— y el seguimiento de páginas oficiales de partidos políticos de extrema derecha. La recolección se limitó a contenido completamente público, dado que los grupos privados requieren aprobación explícita de los administradores para acceder a ellos.

Twitter/X fue monitoreado mediante búsquedas de hashtags y términos específicos, el análisis de cuentas frecuentemente mencionadas en contenidos de otras plataformas y la documentación de hilos de discusión relacionados con eventos extremistas, como manifestaciones o actos violentos. La naturaleza predominantemente pública de la plataforma facilitó el acceso sin necesidad de seguir cuentas específicas.

Los espacios vinculados a los videojuegos emergieron como una categoría adicional durante el proceso de investigación, al documentarse dinámicas de reclutamiento extremista mediante plataformas gaming. Discord, originalmente diseñado para la comunicación entre jugadores, ha sido progresivamente colonizado por comunidades extremistas que crean “servidores” temáticos aparentemente centrados en videojuegos específicos, pero que incluyen canales de discusión política donde se produce una radicalización gradual. Steam, principal plataforma de distribución de videojuegos para PC, permite igualmente la creación de grupos y comunidades

en los que se han identificado espacios extremistas camuflados. Los videojuegos multijugador online, especialmente aquellos con chats de voz escasamente moderados, son señalados recurrentemente como entornos de reclutamiento juvenil. En este sentido, el informe analítico sectorial del EU Knowledge Hub on Prevention of Radicalisation titulado *This Is Not a Game: How Steam Harbors Extremists* (2026) detalla cómo actores radicales instrumentalizan estas comunidades virtuales para normalizar simbología de odio y conectar con perfiles vulnerables. No obstante, el monitoreo exhaustivo de estos espacios resultó limitado en esta investigación, debido a que requieren una participación activa —como integrarse en servidores cerrados de Discord o participar en partidas específicas— que excede los límites metodológicos de una aproximación OSINT puramente observacional.

2. 1 Contexto crítico: evolución del yihadismo digital hacia la "Yihad Blanda"

Antes de detallar la metodología de recogida de datos, resulta fundamental contextualizar una transformación cualitativa del yihadismo digital que condiciona el enfoque de esta investigación y diferencia radicalmente el extremismo religioso contemporáneo del yihadismo clandestino que dominó las dos primeras décadas del siglo XXI.

El yihadismo tradicional operaba mediante un hermetismo deliberado: una comunicación en árabe clásico que funcionaba como barrera lingüística natural, contenidos distribuidos en foros de la dark web inaccesibles para usuarios promedio y códigos teológicos complejos que requerían una formación religiosa especializada para su comprensión. Esta arquitectura cerrada limitaba el alcance a una población específica —mayoritariamente hombres musulmanes arabófonos con conocimientos de jurisprudencia islámica—, pero proporcionaba seguridad operativa mediante la oscuridad y la dificultad de acceso.

Durante los últimos cinco años, diversos análisis de fuerzas de seguridad europeas han documentado la emergencia de un fenómeno denominado internamente **"yihad blanda": una estrategia de radicalización que abandona deliberadamente el hermetismo en favor de la accesibilidad masiva**. Esta transformación no representa una moderación ideológica —el contenido continúa glorificando la violencia, el martirio y el califato—

sino una modernización táctica que adapta el yihadismo a las lógicas de viralización, engagement y economía de la atención que dominan las redes sociales contemporáneas.

Características definitorias de la yihad blanda:

- **Multilingüismo estratégico:** Mientras el yihadismo tradicional asumía que los potenciales reclutas debían aprender árabe como señal de compromiso religioso, la yihad blanda reconoce que esta barrera limita el alcance desproporcionadamente. El contenido se produce sistemáticamente en español, francés, inglés, alemán, y otros idiomas europeos mediante traductores nativos (frecuentemente jóvenes musulmanes europeos de segunda generación radicalizados) o tecnología de traducción asistida por IA. Esta accesibilidad lingüística expande la audiencia potencial desde millones (arabófonos en Europa) a decenas de millones (población total europea).
- **Simplificación discursiva:** La yihad blanda evita la terminología teológica compleja (fiqh, hadith, tafsir, etc.) que requeriría años de estudio para dominar, reemplazándola con narrativas emocionales accesibles: historias personales de “hermanos mártires”, testimonios de “hermanas en califato”, analogías cotidianas que cualquier persona comprende independientemente de formación religiosa. Esta simplificación no constituye un empobrecimiento conceptual accidental, sino una estrategia deliberada para reducir las barreras de acceso a la radicalización.
- **Presencia en plataformas mainstream:** Mientras que el yihadismo clandestino operaba en los foros oscuros de la *dark web* (lo que requería el uso de Tor y un cierto conocimiento técnico), la yihad blanda coloniza deliberadamente Telegram, Instagram (hasta la imposición de los correspondientes bloqueos), TikTok (mediante la evasión de la moderación) y YouTube. Esta elección estratégica reconoce que los jóvenes europeos vulnerables no navegan en la *dark web*, sino que consumen contenido en las aplicaciones que ya tienen instaladas. Telegram proporciona un equilibrio óptimo: está disponible en aplicaciones convencionales (accesibilidad), presenta una interfaz intuitiva (usabilidad) y, al mismo tiempo, ofrece resistencia frente a la moderación gracias a la encriptación y a una jurisdicción escasamente cooperativa.

- Sistema de códigos multimodales: La yihad blanda desarrolla un lenguaje codificado que permite la comunicación de mensajes extremistas, evadiendo la moderación automatizada. Este aspecto se profundiza en la presente investigación.
- Dinámica de grupos de debate temáticos: La yihad blanda organiza canales de Telegram aparentemente centrados en temas legítimos (conflicto palestino-israelí, islamofobia europea, historia colonialismo) que funcionan como embudo de radicalización. El individuo entra buscando información sobre temas de su interés genuino, y gradualmente es expuesto a interpretaciones radicalizadas, luego es invitado a canales más explícitos. Esta arquitectura de escalada gradual mediante intereses comunes replica funnel documentado en extrema derecha (fitness → masculinidad → misoginia → supremacismo).

Esta transformación hacia una “yihad blanda” exige que la investigación no limite el monitoreo a los espacios clandestinos tradicionales, sino que analice también el contenido yihadista presente en plataformas mainstream, donde actualmente opera de forma visible. Adicionalmente, requiere una alfabetización en sistemas de códigos multimodales que permita identificar contenidos que evaden la detección automatizada mediante el uso de emojis, números y audios en lugar de texto explícito, una estrategia que también está presente en otras ideologías extremistas.

Finalmente, existe una marcada asimetría entre la retirada efectiva del contenido yihadista y la persistencia de la propaganda de extrema derecha en internet. El yihadismo es combatido mediante una infraestructura metodológica consolidada por la European Union a través de los Referral Action Days (RADs) de Europol, jornadas de acción coordinada orientadas a identificar y retirar masivamente URLs y contenidos de captación en cuestión de horas. Por el contrario, el extremismo de extrema derecha carece de una arquitectura regulatoria y operativa equivalente a nivel internacional, debido tanto a la ausencia de consenso global sobre su tipificación penal como al uso de narrativas camufladas y ambiguas. Esta carencia de herramientas automatizadas de contención facilita la libre circulación de discursos extremistas en plataformas juveniles, pese a que la extrema derecha representa actualmente el volumen mayoritario del extremismo documentado en redes sociales.

3. Proceso de recolección de datos

El proceso de recolección siguió un protocolo estandarizado para cada publicación identificada como relevante:

Registro de metadatos: Se documentó la URL exacta cuando estaba disponible, nombre de canal/cuenta/usuario, número de seguidores/suscriptores visibles, métricas de engagement (likes, comentarios, shares, visualizaciones), fecha de publicación original cuando era determinable, y contexto de descubrimiento (¿cómo se encontró esta publicación?, ¿búsqueda directa?, ¿recomendación algorítmica?, ¿enlace desde otra plataforma?).

Categorización: Cada publicación fue categorizada según sistema de diecisiete variables desarrollado específicamente para esta investigación.

Almacenamiento: Los datos fueron almacenados en archivos Excel independientes. Este sistema permitió mantener trazabilidad clara de origen mientras facilitaba análisis comparativo posterior. Los archivos fueron almacenados en dispositivo encriptado con acceso restringido mediante contraseña robusta, cumpliendo protocolos de seguridad de datos sensibles.

4. Sistema de categorización

Para garantizar la sistematicidad y replicabilidad del análisis, se desarrolló un sistema de categorización multidimensional que permite clasificar cada unidad de contenido (post, vídeo, mensaje) según 17 variables distintas⁵, organizadas en cuatro dimensiones principales:

Dimensión ideológica. Identifica la corriente extremista predominante (extrema derecha, misoginia/incel, yihadismo, eco-extremismo, conspiracionismo). Esta categoría no es mutuamente excluyente, reconociendo la frecuente convergencia de múltiples odios en un mismo discurso.

Dimensión narrativa. Captura el marco cognitivo (frame) empleado para estructurar el mensaje. Se identificaron 13 narrativas recurrentes, desde el victimismo hasta la criminalización del otro, pasando por la nostalgia del pasado o el mesianismo político del “salvador colectivo”.

5

Para consultar estas variables, véase el apartado metodológico.

Dimensión técnica. Registra el formato (meme, vídeo corto, vídeo largo, texto, etc.), la plataforma de difusión, el nivel de engagement (interacciones), y las tecnologías empleadas (IA generativa, deepfakes, bots, criptomonedas).

Dimensión de riesgo. Evalúa la gravedad del contenido (bajo, medio, alto) atendiendo a criterios como la explicitación de violencia, la especificidad de amenazas, la capacidad de movilización y el potencial de escalada.

Este sistema, desarrollado ad hoc para el presente estudio, integra y adapta marcos conceptuales previos de análisis de extremismo online, incorporando elementos específicamente relevantes para el contexto europeo contemporáneo.

5. Accesibilidad diferencial

Toda la investigación empírica enfrenta limitaciones estructurales que es necesario explicitar para contextualizar adecuadamente los hallazgos. En el presente estudio, la limitación más significativa deriva de la accesibilidad diferencial por ideología.

El **extremismo de extrema derecha** opera mayoritariamente en espacios digitales abiertos o semi-abiertos: Instagram, X, YouTube, y canales públicos de Telegram. Esto permite una monitorización relativamente exhaustiva sin necesidad de infiltración o acceso especializado. Consecuentemente, la muestra de contenido de extrema derecha puede considerarse robusta y representativa del fenómeno.

Las **comunidades misóginas e incel**, aunque frecuentemente operan en canales cerrados de Telegram o foros con acceso restringido, mantienen suficiente presencia en espacios accesibles (Reddit, canales públicos de Telegram, etc) como para permitir una monitorización adecuada, si bien limitada a los contenidos que estas comunidades deciden hacer públicos.

En contraste, el **extremismo yihadista** opera predominantemente en espacios de acceso muy restringido: foros de la dark web, aplicaciones de mensajería cifrada con invitación obligatoria, etc. La monitorización de estos espacios requiere metodologías de infiltración que exceden el alcance

del presente estudio y plantean complejas cuestiones éticas y legales. Para su análisis, nos hemos basado en entrevistas estructuradas con expertos en la materia.

Esta limitación no invalida los hallazgos del estudio, pero sí obliga a circunscribir su alcance y a evitar generalizaciones sobre “extremismo online” que engloben fenómenos que no han sido adecuadamente muestreados.



ANÁLISIS DE RESULTADOS

1. Ecosistema de plataformas digitales del extremismo contemporáneo

El análisis del ecosistema digital extremista revela una arquitectura compleja y estratificada donde diferentes plataformas cumplen funciones específicas dentro de un sistema integrado de radicalización. Lejos de operar de manera aislada, estas plataformas funcionan como red simbiótica donde cada espacio digital desempeña un rol distintivo en el proceso de captación, adoctrinamiento, organización y movilización. El extremismo contemporáneo no habita una única plataforma, sino que construye infraestructura distribuida que explota las características técnicas específicas de cada espacio mientras mitiga sus vulnerabilidades mediante redundancia multi-plataforma.

Este ecosistema puede conceptualizarse como *funnel* de radicalización⁶ con tres niveles funcionales claramente diferenciados. En el nivel superficial operan plataformas mainstream altamente visibles (TikTok, Instagram, YouTube) que funcionan como espacios de captación inicial, exponiendo a audiencias masivas a contenido extremista normalizado, frecuentemente disfrazado de humor, crítica política legítima, o contenido aspiracional sobre masculinidad y superación personal. En el nivel intermedio se sitúan plataformas con moderación laxa o inexistente (Telegram, X bajo gestión Musk, ciertos subreddits) donde ocurre adoctrinamiento sistemático mediante exposición repetida a narrativas extremistas cada vez más explícitas. En el nivel profundo operan espacios completamente cerrados y técnicamente opacos (Discord privado, chats cifrados, foros dark web, servidores gaming privados) donde se desarrolla planificación operativa, coordinación de acciones, y radicalización final hacia violencia.

La transición entre niveles no es accidental sino cuidadosamente orquestada. Los contenidos virales en TikTok incluyen discretamente referencias a “seguir conversación en Telegram” mediante códigos en *caption*⁷ o enlaces en biografía. Las cuentas de Instagram con decenas de miles de

6 Proceso gradual de captación que funciona como un embudo, donde individuos son atraídos inicialmente mediante contenido aparentemente inocuo o de interés general (la “boca” amplia del embudo) y progresivamente expuestos a contenido cada vez más extremo y radicalizado (el “cuello” estrecho del embudo).

7 Texto descriptivo que acompaña una publicación en redes sociales y que contiene lenguaje codificado (números, emojis, términos encubiertos) para comunicar mensajes extremistas evadiendo la moderación automatizada de plataformas.

seguidores direccionan sistemáticamente hacia canales de Telegram mediante mensajes directos a usuarios que comentan con entusiasmo. Los videos de YouTube incluyen enlaces a Discord “para comunidad más activa”. Esta arquitectura de embudo evidencia una sofisticación estratégica considerable: el extremismo digital contemporáneo no espera a que las audiencias busquen contenido radical, sino que construye canales automatizados que conducen progresivamente a los usuarios desde el contenido común hacia espacios cada vez más extremos.

El análisis detallado de las ocho categorías principales de plataformas monitoreadas durante esta investigación revela las características específicas, funciones dentro del ecosistema, y dinámicas de radicalización propias de cada espacio.

MODELO DE EMBUDO DE RADICALIZACIÓN DIGITAL

NIVEL 1: SUPERFICIAL

[Captación inicial masiva]

Plataformas	TikTok, Instagram, YouTube
Características	Altamente visibles y mainstream. Audiencias masivas. Contenido extremista normalizado.
Camuflaje	Humor, memes. Crítica política aparentemente legítima. Contenido aspiracional [masculinidad, superación personal].

NIVEL 2: INTERMEDIO

[Adoctrinamiento sistemático]

Plataformas	Telegram, X (bajo gestión Musk), ciertos subreddits
Características	Moderación laxa o inexistente Exposición repetida a narrativas extremistas Contenido progresivamente más explícito
Proceso	Normalización de discursos radicales Construcción de identidad grupal Escalada gradual de extremismo

NIVEL 3: PROFUNDO

[Planificación operativa y radicalización final]

Plataformas	Discord privado, chats cifrados, foros dark web, servidores gaming privados
Características	Completamente cerrados Técnicamente opacos Acceso restringido
Actividades	Planificación operativa de acciones Coordinación de ataques Radicalización final hacia violencia



1.1 Telegram: epicentro operativo del extremismo digital

Telegram emergió durante esta investigación como la plataforma central del extremismo de ideologías pertenecientes a la extrema derecha e incels en el medio digital europeo contemporáneo, funcionando simultáneamente como espacio de difusión masiva, organización logística, construcción de comunidad, y coordinación transnacional. Esta aplicación de mensajería, diseñada originalmente con énfasis en la privacidad y cifrado punto a punto, ha sido progresivamente colonizada por actores extremistas expulsados de otras plataformas con mayor moderación, convirtiéndose en refugio de facto para un tipo de contenido que sería inmediatamente eliminado en espacios más regulados.

La arquitectura técnica de Telegram facilita esta función mediante varias características distintivas. La estructura de “canales” permite difusión unidireccional de contenido a audiencias masivas (decenas de miles de suscriptores en algunos casos analizados) sin posibilidad de moderación externa, ya que Telegram no implementa sistemas automatizados de detección de contenido extremista y raramente responde a reportes de usuarios. Los “grupos” complementan esta función permitiendo discusión bidireccional y coordinación operativa entre miembros, pudiendo alcanzar hasta doscientos mil participantes. La capacidad de compartir archivos de cualquier tipo y tamaño sin restricción facilita distribución de manuales extremistas, propaganda diseñada profesionalmente, y documentación de actividades.

Crucialmente, Telegram cultiva una reputación de plataforma “segura” y “privada” mediante una estrategia de comunicación que enfatiza su resistencia a la censura gubernamental, aunque la realidad técnica se puede matizar. Como ejemplo de esta proyección corporativa, el fundador de la aplicación, Pável Dúrov (fundador de Telegram), remitió un mensaje masivo directo a los teléfonos de todos los usuarios de la plataforma en España. En dicha declaración oficial, Dúrov arremetió contra los planes del Gobierno para limitar el acceso a las redes sociales a menores de 16 años, tachando la iniciativa de “regulación peligrosa” y alertando del riesgo de transformar el país en un “estado de vigilancia bajo el pretexto de protección” (Durov, 2026). Esta instrumentalización de la infraestructura privada para ejercer influencia política directa evidencia cómo la firma prioriza su narrativa

autocensura sobre las demandas estatales de protección de la infancia. Los canales públicos monitoreados en esta investigación no están cifrados; cualquier persona con enlace puede acceder y todo contenido es técnicamente visible para los administradores de Telegram. Sin embargo, la percepción de privacidad genera una confianza que reduce las inhibiciones, mientras que la resistencia histórica de Pavel Durov a cooperar con las autoridades europeas proporciona una garantía práctica: el contenido extremista no será eliminado de manera sistemática.

Durante el período de investigación, se monitorearon diversos canales principales de Telegram, abarcando el espectro completo del extremismo accesible. ISL Paladins representó un caso paradigmático de sofisticación organizativa transnacional, operando mediante la newsletter semanal Sunday Digest, que alcanzaba los novecientos veintiocho suscriptores directos, aunque con una circulación estimada mucho mayor mediante el reposteo. El canal no solo difundía propaganda, sino que coordinaba eventos internacionales, distribuía invitaciones al Foro de San Petersburgo y mantenía vínculos formales con quince organizaciones en múltiples países. El contenido combinaba la explotación sistemática de crímenes individuales cometidos por migrantes para construir la narrativa del “Gran Reemplazo”⁸ con una teorización política explícita sobre la incompatibilidad racial absoluta y la necesidad de la “remigración” (deportación masiva).

Los canales de extrema derecha española documentados operaban mediante una combinación de contenido ideológico denso (series completas sobre la “etnopolítica” nacional-socialista) con amenazas específicas contra individuos identificables, como el futbolista Iñaki Williams, amenazado con una futura expulsión bajo un “Estado Nacionalista”. El canal *Ad Victoriam* ejemplificó el neonazismo explícito mediante laglorificación del cumpleaños de Hitler, presentada como una biografía hagiográfica de “el cabo” (eufemismo empleado para evadir la detección), la conmemoración de la quema de libros nazis de 1933 como un acto de “formación de una sociedad sana”, y un antisemitismo sistemático basado en la difusión de teorías conspirativas sobre el control judío de las finanzas y los medios de comunicación. Significativamente, *Ad Victoriam* operaba con infraestructura multi-plataforma abarcando siete

8 Teoría conspirativa de corte supremacista que afirma la existencia de un plan coordinado por élites políticas y económicas para reemplazar a la población nativa de los países occidentales mediante la inmigración masiva (Center on Extremism, 2022). La literatura científica identifica esta narrativa como el elemento motivacional común en múltiples atentados de la última década, operando como el puente ideológico entre el discurso político radical común y la acción terrorista violenta.

espacios digitales incluyendo PayPal para crowdfunding público, evidenciando la profesionalización y el financiamiento activo.

El Centro Studi Fascismo italiano representó un caso distintivo de extremismo que opera bajo la cobertura de una “asociación cultural”, glorificando el régimen de Mussolini mediante un archivo de propaganda de la República Social Italiana (estado títere nazi entre 1943 y 1945), la celebración de la Marcha sobre Roma como momento fundacional y la reivindicación explícita de un “Estado totalitario” sin eufemismos. Blocco Studentesco, la rama juvenil del partido neofascista CasaPound, mantenía un canal principal con cinco mil seiscientos cincuenta y cinco suscriptores, además de subgrupos regionales, coordinando manifestaciones simultáneas en múltiples ciudades italianas y organizando actividades físicas (boxeo y eventos sociales) que contribuían a la construcción de una comunidad cohesionada.

Un canal incel monitoreado operaba mediante una memificación total, donde el cien por cien del contenido consistía en imágenes manipuladas que promovían la misoginia extrema. La glorificación explícita de Elliot Rodger (terrorista del ataque de la Isla Vista en 2014) mediante publicaciones que proclamaban “*will always stay by your side*” representó el caso más grave de apología del terrorismo documentado. El nombre de usuario del administrador, “*broken_rape_victim*”, glorificaba la violencia sexual, mientras que el contenido normalizaba la ideación suicida mediante un humor negro repetitivo.



Figura 1. Captura de chat con contenido incel accesible a todos los usuarios.

Fuente: Telegram.

Las redes Antifa documentadas en el canal "Antifa Squads" presentaban un caso distintivo de extremismo de extrema izquierda transnacional que celebraba la violencia física con una franqueza inusual, describiendo confrontaciones específicas en Clermont ("once antifas versus ocho fascistas", "*distribution de patates de forains et de pénalty*"), Roma ("cuatro antifas versus nueve fascistas de Forza Nuova"), Burdeos ("*coup de poubelles*") y Toulouse (tres días de acoso sistemático, denominado "*bolossage*"). La red operaba mediante las "*connexions*" coordinadas entre grupos ubicados en Francia, Italia, Alemania, Grecia, Australia e Irlanda.

1.2 Instagram: red de amplificación viral y puerta de entrada

Instagram opera como un ecosistema de amplificación viral para el extremismo de derecha español, funcionando mediante una red coordinada de cuentas que ejecutan una estrategia deliberada de normalización y captación masiva. Aunque la plataforma implementa políticas de moderación formalmente más restrictivas que Telegram, el análisis reveló que su algoritmo de recomendación amplifica activamente el contenido extremista debido a que este genera un elevado *engagement* (likes, comentarios, comparticiones y tiempo de visualización), métrica que el sistema prioriza sin una evaluación del impacto social o de la veracidad.

El formato de los Reels (vídeos cortos de entre 15 y 90 segundos) ha sido especialmente efectivo para la difusión viral de narrativas extremistas mediante una estética profesional y una producción de alta calidad. Los vídeos combinan imágenes impactantes, música emocional y texto superpuesto con mensajes simplificados, y recurren frecuentemente al humor o a la ironía, que funcionan como un escudo frente a las acusaciones de extremismo («es solo una broma»). Esta presentación sofisticada contrasta marcadamente con el estereotipo del contenido extremista como contenido amateur y visualmente tosco.

Instagram resulta especialmente relevante para los grupos yihadistas, que han identificado la plataforma como un espacio estratégico para la captación inicial mediante el uso de *nasheeds* (cánticos vocales islámicos sin instrumentos musicales) integrados en los Reels. Esta investigación profundiza más adelante en los códigos y las herramientas empleadas, pero la combinación de imágenes de batallas históricas islámicas, texto en árabe

con traducción al español y un *nasheed* emocionalmente intenso genera una elevada atracción viral entre los jóvenes musulmanes europeos que consumen dichos Reels como entretenimiento, sin reconocer inicialmente la función propagandística del contenido.

La investigación identificó una red coordinada de seis cuentas principales vinculadas mediante el análisis de *hashtags* compartidos, el *timing* sincronizado de las publicaciones, las menciones cruzadas y, de manera crucial, la frase repetida "*and two/three others*", que aparecía en múltiples publicaciones e indicaba una coordinación explícita.

El contenido de una cuenta española que se presentaba como medio de comunicación abarcó la glorificación de una manifestación de ultraderecha en Polonia, con cientos de miles de asistentes bajo el eslogan "RECONQUISTA"; el ataque contra una "adoctrinadora LGTBI+", reclamando la retirada de la custodia del menor; y una campaña coordinada de "REMIGRACIÓN" en Inca (Mallorca) mediante la colocación masiva de pegatinas durante la noche. Otra cuenta, perteneciente a un "influencer", presentó un caso distintivo de creador de contenido de origen camerunés que promovía la ultraderecha antiinmigración, funcionando como un "token" legitimador. En ella convergían la misoginia explícita ("nacionalista del chumino") con la victimización de Luis Rubiales, condenado por la Audiencia Nacional por agresión sexual.

Instagram actúa típicamente como una puerta de entrada dentro de una arquitectura de funnel multiplataforma. Los usuarios son inicialmente expuestos a contenido extremista de baja intensidad mediante el algoritmo de recomendación, que identifica a los usuarios susceptibles basándose en sus interacciones previas —seguimiento de cuentas conservadoras o likes en contenido relacionado con la "tradición" o la "familia"—. Posteriormente, el sistema les muestra contenido progresivamente más explícito y, aquellos que demuestran un interés sostenido, son redirigidos hacia Telegram mediante enlaces en las biografías de los perfiles o mensajes directos automatizados. Esta transición suele producirse cuando el usuario comenta en múltiples ocasiones o comparte contenido, señalando un grado de compromiso que trasciende el mero consumo pasivo.

1.3 Reddit: intelectualización pseudoacadémica del odio

Reddit alberga comunidades extremistas con características distintivas que las diferencian cualitativamente de las manifestaciones observadas en otras plataformas. A diferencia de los espacios donde el contenido es predominantemente visual —memes en los canales incel de Telegram o vídeos cortos en Instagram—, Reddit privilegia el formato de texto largo, lo que permite la construcción de narrativas complejas, la elaboración de argumentos y el desarrollo de un corpus pseudointelectual que presenta el extremismo como una posición razonada, en lugar de como un prejuicio de carácter emocional.

Los subreddits específicos funcionan como espacios de refuerzo mutuo donde la ideología es constantemente reafirmada mediante discusión aparentemente racional. El subreddit r/DebateIncelz, nominalmente dedicado a “debatir ideología incel”, opera en realidad como echo-cámara⁹ sofisticada donde cuestionamientos genuinos son marginalizados mediante downvotes¹⁰ mientras que las afirmaciones de ideología Blackpill son sistemáticamente apoyadas y premiadas. El anonimato total de la plataforma (usuarios identificados únicamente por username sin vinculación a identidad real) reduce inhibiciones, permitiendo la expresión de contenido que usuarios no compartirían en redes como Facebook vinculadas a nombre real.

El análisis de *threads* (hilos) específicos reveló dinámicas preocupantes. El debate sobre “¿cuánto tiempo celibato para ser truecel again? (sic)” documentó gatekeeping¹¹ extremo donde la comunidad establece criterios

9 Espacio virtual cerrado donde las opiniones y creencias de un usuario son amplificadas y reforzadas por la repetición constante, quedando excluidas las posturas alternativas (Sunstein, 2017). Los algoritmos de recomendación de contenidos masivos crean estas dinámicas al indexar los perfiles de los usuarios en bucles de retroalimentación de información extremista, lo que neutraliza el pensamiento crítico y facilita la inmersión profunda en discursos radicalizados.

10 Upvotes y Downvotes: Sistema de votación de Reddit donde usuarios pueden votar positivamente (upvote, flecha arriba) o negativamente (downvote, flecha abajo) publicaciones y comentarios. Este mecanismo permite que comunidades extremistas amplifiquen contenido radical mediante upvotes masivos coordinados y silencien voces disidentes mediante downvotes, creando cámaras de eco donde solo narrativas extremistas dominan.

11 El gatekeeping se refiere al proceso mediante el cual los miembros consolidados de una subcultura o comunidad ejercen el control de acceso a la misma, imponiendo barreras normativas y exigencias de identidad para validar la legitimidad de sus integrantes (Sugiura, 2021). En los entornos radicales y de la manosfera, esta vigilancia de fronteras grupales radicaliza el discurso al castigar la moderación y recompensar la adopción de posturas cada vez más extremas, exigiendo pruebas constantes de sufrimiento colectivo para otorgar el estatus de miembro auténtico o truecel.

de pureza ideológica, determinando colectivamente quién califica como incel “auténtico” versus “falso”. Los comentarios más votados afirmaban que experiencia sexual es contaminación permanente (*“like virginity, once it’s gone it’s gone”* con diecinueve upvotes), estableciendo la identidad incel como un estatus irrevocable similar a conversión religiosa.

El hilo titulado “Experiencias con Chad” (*“Experiences with Chad”*) representó el contenido más grave mediante la normalización del antisemitismo casual. El comentario que describía a un “nazi tierno” (*“uwu Nazi”*) que “hacía chistes sobre judíos constantemente” (*“constantly made jokes about jews”*) y simultáneamente “se acostaba con múltiples chicas” (*“slept with multiple girls”*) —el cual recibió veinte votos a favor (upvotes)— presentaba el antisemitismo y el éxito social como elementos compatibles, sin que mediara ninguna condena moral por parte de la comunidad. Otro comentario sobre *“neo nazi who looks like tiktok pretty boy”* que *“genuinely has no problem getting laid including by brown women”* versus *“short unattractive very left wing very feminist friend struggles”* (tres upvotes) articulaba el determinismo biológico extremo: apariencia supera ideología, moralidad es irrelevante, solo la genética determina el valor.

El *thread* sobre los *“triggers”* documentó una crisis de salud mental colectiva mediante la descripción de síntomas compatibles con un trastorno de estrés postraumático. Un usuario de treinta años describía una respuesta fisiológica extrema —taquicardia, sensación de cierre de la garganta, hormigueo en los brazos y la percepción de que *“whole body feels activated”* durante períodos de entre treinta minutos y varias horas— desencadenada por el hecho de *“hearing or reading a woman express her attraction for a man”*. Los comentarios revelaron la normalización de la ideación suicida, con un usuario sugiriendo que un hombre discapacitado de cincuenta años y virgen debería considerar el *“assisted suicide”*, comentario que recibió respuestas de apoyo y acuerdo, sin encontrar oposición.

La sofisticación del discurso en Reddit, empleando terminología pseudo-científica (*“determinismo biológico”, “lookism”, “hypergamy”*), vocabulario académico (*“evolutionary psychology”, “sexual market value”*), y referencias a estudios científicos frecuentemente malinterpretados o descontextualizados, confiere un barniz de legitimidad intelectual a misoginia extrema. Esta presentación “racional” resulta particularmente efectiva para la radicalización

de hombres jóvenes educados que podrían rechazar la misoginia presentada mediante memes crudos, pero son susceptibles a argumentos que aparentan rigor científico.

1.4 TikTok: captación masiva de audiencia juvenil vulnerable

TikTok representa el principal vector de captación juvenil del extremismo contemporáneo, exponiendo a audiencias mayoritariamente adolescentes y jóvenes adultas (de doce a veintiocho años) a un contenido extremista normalizado mediante una estética aspiracional y un humor transgresor. Con más de mil millones de usuarios activos mensuales y una demografía fuertemente concentrada en menores de veinticinco años, la plataforma proporciona un acceso sin precedentes a una generación en proceso de formación de identidad política y particularmente vulnerable a la influencia.

Los videos de quince a sesenta segundos permiten la difusión de mensajes extremistas radicalmente simplificados, despojados de contexto o de matización, frecuentemente presentados mediante la ironía o la sátira, lo que evade tanto la moderación automatizada como la resistencia psicológica del espectador. Un video puede comunicar una narrativa completa del “Gran Reemplazo” en treinta segundos mediante una secuencia de imágenes de migrantes, estadísticas descontextualizadas sobre demografía, música dramática y el texto “Despierta”¹², sin articular explícitamente una teoría conspiratoria, permitiendo una negación plausible si es reportado.

El algoritmo de TikTok, diseñado para maximizar el tiempo de uso mediante recomendaciones hiperpersonalizadas que aprenden las preferencias del usuario extremadamente rápido, tiende a crear “burbujas de filtro” donde los usuarios inicialmente expuestos a contenido levemente transgresor son progresivamente derivados hacia contenido cada vez más extremo. Este fenómeno de “rabbit hole” algorítmico opera automáticamente: un adolescente que visualiza un video sobre “masculinidad tradicional” verá recomendaciones sobre “el feminismo destruye la sociedad”, que conducen a

¹² Término utilizado por comunidades extremistas (especialmente extrema derecha) como llamado a «despertar» del supuesto engaño de narrativas mainstream sobre inmigración, feminismo, diversidad o globalización, presentándose como portadores de «verdad oculta» que masas “dormidas” ignoran. Implica que adherirse a extremismo es acto de consciencia y lucidez versus “adoctrinamiento” de medios y sistema educativo.

“las mujeres solo quieren hombres ricos”, derivando finalmente en contenido explícitamente misógino incel, todo ello en una sesión de scrolling de treinta minutos.

La estética “sigma/grindset” ha sido particularmente efectiva en TikTok como vehículo de radicalización camuflada. Los videos que presentan rutinas de ejercicio intenso, consejos de productividad, citas sobre auto-mejora y la mentalidad de “lobo solitario” atraen inicialmente mediante la apariencia de contenido motivacional legítimo. Progresivamente, estos contenidos introducen elementos de masculinidad tóxica: el rechazo de las emociones como debilidad, la presentación de las relaciones como transacciones donde las mujeres son recursos a optimizar, la glorificación de la dominancia y

la agresividad y, eventualmente, narrativas explícitas sobre la “naturaleza femenina” y el determinismo biológico del género.

El cross-posting documentado entre TikTok e Instagram evidencia una estrategia deliberada multi-plataforma. El contenido viral en TikTok (videos que alcanzan millones de visualizaciones) es repostado en Instagram preservando la marca de agua de TikTok, donde alcanza a una audiencia diferente y genera tráfico de retorno hacia TikTok mediante la curiosidad sobre la fuente original. Simultáneamente, los creators incluyen enlaces a Telegram en la biografía de TikTok, permitiendo que los usuarios más comprometidos accedan a contenido sin restricciones de moderación.

1.5 YouTube: adoctrinamiento sistemático en formato largo

YouTube mantiene su rol histórico como plataforma privilegiada para el adoctrinamiento sistemático mediante contenido de formato largo que permite el desarrollo gradual de narrativas complejas. Mientras que otras redes sociales han evolucionado hacia un contenido cada vez más breve y fragmentado (stories de quince segundos, reels de treinta segundos y tweets de doscientos ochenta caracteres), YouTube permite la construcción de “cursos” completos de ideología extremista mediante series de videos de treinta minutos a dos horas que guían metódicamente al espectador desde posiciones inicialmente moderadas hacia posiciones progresivamente radicales.

El fenómeno del “redpilling” (el adoctrinamiento gradual presentado como un “despertar” a verdades ocultas que la sociedad mainstream oculta) encuentra en YouTube su medio ideal. Las series identificadas desarrollan conceptos de “etnopolítica” nacional-socialista que operan mediante una estructura curricular que mimetiza la educación formal: un episodio introductorio establece los conceptos básicos, los episodios subsecuentes profundizan en temas específicos (“Blut und Boden” —sangre y suelo—) y la serie completa construye un corpus ideológico coherente. La duración permite no solo la afirmación de ideas, sino también una argumentación extensa, la refutación preventiva de objeciones anticipadas y una contextualización histórica que confiere una apariencia de rigor académico.

La estética visual es crucial para la efectividad del adoctrinamiento en YouTube. Los canales más sofisticados emplean una producción profesional con iluminación de calidad, edición pulida, gráficos informativos, música de fondo que genera una atmósfera apropiada y presentadores articulados que proyectan autoridad intelectual. Esta inversión en producción diferencia el contenido extremista contemporáneo de la propaganda amateur de décadas previas, haciendo que los videos aparenten ser documentales legítimos de historia o análisis político serio, en lugar de rants conspirativos de individuos marginales.

El sistema de recomendación algorítmica de YouTube ha sido ampliamente documentado en investigaciones previas como un vector de radicalización, conduciendo a los usuarios desde el contenido mainstream hacia el extremismo mediante una sucesión de recomendaciones progresivamente más radicales. Aunque YouTube implementó medidas correctoras en años recientes (reduciendo las recomendaciones de contenido “borderline”, promoviendo fuentes autoritativas para temas sensibles y añadiendo paneles informativos a videos sobre eventos de actualidad), el análisis reveló que el contenido extremista persiste mediante la evasión táctica: los canales evitan palabras clave que activan restricciones, presentan el contenido extremista como un “análisis histórico objetivo” u operan mediante una red de canales pequeños que vuelan bajo el radar de la moderación.

Los comentarios en los videos de YouTube funcionan como un espacio complementario de construcción de comunidad y refuerzo ideológico. A

diferencia de otras plataformas en las que los comentarios son efímeros y desorganizados, YouTube permite “hilos” de discusión extensos donde los usuarios debaten, comparten recursos adicionales y se reconocen mutuamente como comunidad. Los creadores de contenido frecuentemente participan en los comentarios, generando una sensación de acceso directo al “líder intelectual” del movimiento. Este aspecto comunitario transforma el consumo pasivo de video en una participación activa en el movimiento.

1.6 Facebook: declive relativo pero persistencia institucional

Facebook mantiene una presencia relevante, aunque cuantitativamente decreciente, en el ecosistema extremista europeo contemporáneo. Asociada demográficamente a usuarios de mayor edad (treinta y cinco años en adelante), la plataforma concentra especialmente contenido de ultraderecha institucional vinculado a partidos políticos formales y teorías conspirativas sobre temas mainstream (las vacunas, las elecciones y la inmigración).

Las “páginas” de Facebook permiten la agregación de audiencias masivas bajo una identidad organizacional sin necesidad de reciprocidad (los usuarios pueden seguir una página sin que la página los siga de vuelta, a diferencia de las amistades que requieren una aceptación mutua). Las páginas de AfD monitoreadas alcanzaban decenas de miles de seguidores, permitiendo una difusión unidireccional similar a los canales de Telegram, pero con una mayor legitimidad percibida por operar en una plataforma mainstream. Los “grupos” complementan esta función permitiendo la discusión entre miembros, aunque la moderación de Facebook ha mejorado significativamente en años recientes, expulsando hacia Telegram a los actores más explícitamente extremistas.

El contenido en Facebook tiende a ser menos explícitamente extremista que en Telegram, pero más sofisticado en su empaquetado. Mientras que Telegram permite la glorificación abierta de Hitler o la celebración de la violencia, Facebook requiere una mayor sutileza: el mismo contenido es presentado mediante preguntas retóricas (“¿por qué no podemos discutir...?”), apelaciones a la libertad de expresión (“nos quieren silenciar”) o enmarcado como una preocupación legítima (“solo queremos proteger nuestros valores”). Esta moderación forzada genera el desarrollo de un lenguaje codificado y de narrativas más elaboradas que, paradójicamente, pueden ser más efectivas para la radicalización de audiencias moderadas que rechazarían el extremismo explícito.

1.7 X (Twitter): difusión rápida y debate polarizado

X (anteriormente Twitter) funciona como una plataforma de difusión rápida, construcción de narrativas virales y debate público altamente polarizado. Bajo la gestión de Elon Musk desde octubre de 2022, la plataforma ha experimentado una transformación significativa en sus políticas de moderación, permitiendo el retorno de cuentas previamente suspendidas por violación de políticas contra el discurso de odio, relajando el enforcement de las reglas existentes y promoviendo una ideología de “libertad de expresión absolutista” que, en la práctica, ha resultado en la proliferación de contenido previamente prohibido.

El formato de mensajes breves (originalmente de ciento cuarenta caracteres, expandido a doscientos ochenta y actualmente permitiendo posts largos para suscriptores premium) favorece la simplificación extrema, las declaraciones categóricas sin matización y la polarización, debido a la imposibilidad de desarrollar argumentos complejos. El sistema de “trending topics” y el feed “For You” amplifican el contenido controvertido que genera un alto engagement, creando un incentivo perverso donde la provocación extrema es recompensada con una visibilidad masiva.

Durante el período de investigación, se observó un uso estratégico de X para la difusión de convocatorias a eventos físicos (manifestaciones de ultraderecha y concentraciones identitarias), la coordinación de campañas de acoso dirigido contra individuos específicos mediante “brigading” (cientos de usuarios atacando simultáneamente a un objetivo) y la construcción de narrativas de victimización que presentan las restricciones moderadas de contenido como una “censura totalitaria”, comparando a las plataformas con regímenes autoritarios.

El caso documentado de Comte de Descatllar (@MAFMT83) tuiteando “Tic-tac, marrons, us substituirem per robots” ejemplifica el uso de un insulto racial explícito (“marrons”, refiriéndose a personas racializadas) combinado con una amenaza de reemplazo, que posteriormente circuló como screenshot en Instagram alcanzando una audiencia amplificada. Esta dinámica de “screenshot journalism”, donde el contenido de X es capturado y redistribuido en otras plataformas, extiende el alcance más allá de los usuarios directos de X.

1.8 Espacios de videojuegos: vector emergente de reclutamiento juvenil

Los espacios digitales asociados con videojuegos emergieron durante esta investigación como vector significativo, aunque frecuentemente subestimado de reclutamiento extremista juvenil. Plataformas diseñadas originalmente para comunicación entre jugadores han sido progresivamente colonizadas por actores extremistas que explotan características específicas de estos espacios: demografía mayoritariamente masculina y joven, cultura de transgresión normativa donde “humor ofensivo” es normalizado, anonimato que reduce inhibiciones, y vínculos comunitarios fuertes desarrollados mediante juego colaborativo.

Discord, aplicación de comunicación por voz y texto diseñada para coordinación en videojuegos multijugador, representa un caso paradigmático de colonización extremista de infraestructura gaming. La plataforma opera mediante “servidores” privados que los propietarios crean y administran con control total sobre membresía, estructura de canales, y reglas. Grupos extremistas crean servidores temáticos aparentemente dedicados a juegos específicos populares (Minecraft, Fortnite, Call of Duty, League of Legends) pero que incluyen canales de discusión “off-topic” donde se produce la radicalización gradual.

La arquitectura típica de servidor Discord extremista camuflado incluye canales públicos sobre gaming (discusión de estrategias, búsqueda de compañeros de equipo, compartir clips de jugadas) que atraen usuarios legítimos, canales semi-públicos sobre temas políticos presentados inicialmente como “debate libre” donde se introduce contenido progresivamente extremo, y canales privados accesibles únicamente mediante promoción basada en demostración de compromiso ideológico donde ocurre planificación operativa y radicalización final. Este sistema de capas permite reclutamiento gradual: jugador joven se une para discutir videojuegos, es expuesto a “memes políticos” en canal general; si demuestra receptividad, es invitado a canales más exclusivos.

La comunicación por voz en Discord añade la dimensión de intimidad ausente en plataformas de solo texto. Sesiones de gaming donde los usuarios juegan juntos durante horas mientras conversan por voz y crean vínculos personales fuertes. Los extremistas explotan estos vínculos mediante la estrategia de “ser amigable primero, radicalizar después”: establecen

relaciones genuinas mediante gaming colaborativo, generan confianza y lealtad, y posteriormente introducen contenido ideológico presentado como opiniones personales de “amigo” en lugar de propaganda de extraño.

Steam, plataforma dominante de distribución de videojuegos para PC con más de ciento veinte millones de usuarios activos, permite la creación de “grupos” y “comunidades” donde se documentaron espacios extremistas camuflados. Grupos con nombres aparentemente benignos dedicados a juegos históricos (simuladores de Segunda Guerra Mundial, juegos de estrategia histórica) incluían foros donde usuarios glorificaban figuras históricas extremistas, compartían propaganda, y reclutaban hacia espacios externos. El sistema de “curadores” de Steam, donde usuarios recomiendan juegos a seguidores, ha sido explotado por extremistas para construir audiencias que posteriormente son direccionadas hacia contenido político.

Los juegos online multijugador con sistemas de chat de voz no moderado funcionan como espacios de exposición a un lenguaje extremista normalizado. Investigaciones previas documentan la prevalencia de insultos raciales, misoginia extrema y humor sobre el Holocausto en los chats de voz de títulos competitivos populares como Counter-Strike, League of Legends o Call of Duty. Estas conductas suelen ser justificadas como “parte de la cultura gaming” y defendidas bajo el argumento de que “es solo una broma” o el “tradicional trash talk” (charla basura). No obstante, esta problemática excede el plano puramente verbal: plataformas de apariencia infantil y masiva como Roblox sufren la modificación deliberada de sus escenarios para introducir simbología y narrativas yihadistas complejas, convirtiendo entornos recreativos comunes en potentes focos de adoctrinamiento visual (Pérez-García y Barragán, 2025). Para adolescentes que pasan decenas de horas semanales en estos entornos, la exposición repetida normaliza lenguaje y actitudes extremistas, reduciendo el umbral de shock y creando familiaridad que facilita radicalización posterior.



Figura 2. Captura de chat con contenido Incel y Gamer accesible a todos los usuarios. **Fuente:** Telegram.

La integración del streaming (Twitch y YouTube Gaming) añade una capa adicional de influencia. Los streamers populares, con audiencias de decenas de miles de espectadores simultáneos, funcionan como figuras de autoridad para la audiencia joven. Los streamers que expresan opiniones políticas extremistas “casualmente” durante las sesiones de gaming, presentadas como opiniones personales espontáneas en lugar de contenido político deliberado, ejercen una influencia considerable. La parasocial relationship (la sensación de amistad unilateral que los espectadores desarrollan con los streamers que observan regularmente) amplifica el impacto: un adolescente vulnerable percibe una opinión extremista no como la propaganda de un activista político, sino como la perspectiva de un “amigo” admirado.

Este vector de radicalización mediante los espacios gaming resulta particularmente preocupante porque opera bajo el radar de padres, educadores y, frecuentemente, investigadores. Mientras existe una conciencia creciente sobre el extremismo en las redes sociales tradicionales, los espacios gaming son percibidos como un entretenimiento inocuo. Los padres que monitorizan cuidadosamente el Facebook e Instagram de sus hijos pueden estar completamente inconscientes de la exposición al extremismo en Discord o

en los chats de voz durante las sesiones de Fortnite presentadas como “jugar con amigos”.¹³

ANÁLISIS INTEGRAL MONITOREO EXTREMISMO ONLINE	
PLATAFORMAS MONITOREADAS	
PLATAFORMA	NIVEL DE RIESGO
TELEGRAM	CRÍTICO
INSTAGRAM	ALTO
REDDIT	ALTO
FACEBOOK	MEDIO
YOUTUBE	MEDIO
TWITTER / X	MEDIO
TIKTOK	ALTO

Figura 3. Cuadro-resumen del nivel de riesgo en cada una de las plataformas analizadas. **Fuente:** elaboración propia.

2. Códigos, lenguaje y símbolos identificados

2.1 Extrema Derecha: descodificando

El discurso de extrema derecha online ha desarrollado un complejo sistema de códigos lingüísticos que cumple una doble función: por un lado, permite la comunicación intragrupal evitando la moderación de plataformas; por otro, funciona como marcador de pertenencia e iniciación que distingue a “iniciados” de “externos”.

Los términos de **gravedad crítica** representan aquellos que, en su mera enunciación, indican un nivel de radicalización avanzado y constituyen señales de alerta máxima:

“Remigración” se ha consolidado como el eufemismo preferido para referirse a la deportación masiva de poblaciones migrantes y sus

13 Otros espacios: Hay una creciente preocupación adicional por contenido extremista cada vez más frecuente en otros formatos de ocio, como pueden ser canciones o podcasts que se encuentran en plataformas online abiertas (Spotify, Apple Music,etc).

descendientes. Originado en círculos identitarios franceses y austriacos, el término presenta la expulsión forzosa de millones de personas como una política gestionable y necesaria, evitando la asociación directa con conceptos históricos como “limpieza étnica” o “deportación”. Durante el período de estudio, “remigración” aparece de forma transversal en contenido español, italiano, francés y alemán, indicando su consolidación como narrativa paneuropea de la extrema derecha. Su uso ha trascendido círculos marginales para aparecer en discurso de partidos con representación parlamentaria, normalizando progresivamente lo que hace una década sería considerado discurso extremista inaceptable.

“El Cabo” representa un ejemplo paradigmático de evasión lingüística. Dado que la mención explícita de “Hitler” activa frecuentemente mecanismos de moderación automática, actores extremistas españoles han adoptado esta referencia oblicua basada en el rango militar de Hitler durante la Primera Guerra Mundial. El término permite referencias laudatorias, nostálgicas o reivindicativas del nazismo sin pronunciar el nombre explícito, evadiendo tanto la detección algorítmica como, en algunos contextos, las posibles consecuencias legales por apología del nazismo. La proliferación de este código indica un nivel de sofisticación en las estrategias de evasión.

“Marrons” constituye un insulto racial de uso específico en círculos ultra-derechistas catalanes y españoles, dirigido contra personas racializadas, especialmente de origen africano o latinoamericano. Su función es la deshumanización mediante la reducción de personas a una característica física expresada de forma peyorativa. El término circula principalmente en canales abiertos (Telegram, Youtube, TikTok, etc.) y grupos privados, donde la moderación es inexistente.

Los términos de **gravedad alta** indican radicalización significativa sin alcanzar el umbral crítico:

“Lügenpresse” (“prensa mentirosa” en alemán) tiene una carga histórica específica: fue utilizado masivamente por la propaganda nazi para deslegitimar medios de comunicación independientes. Su reaparición en el discurso de AfD y grupos ultraderechistas alemanes contemporáneos no es casual, sino una recuperación deliberada de la terminología del Tercer Reich. El término ha sido adoptado también en otros contextos europeos (traducido como “prensa mentirosa”, “fake news”, etc.) como parte de una estrategia sistemática de deslegitimación de instituciones democráticas.

“Reconquista” evoca las Cruzadas medievales y la expulsión de musulmanes de la Península Ibérica, presentando la actual presencia musulmana en Europa como una “invasión” que requiere una nueva “reconquista”. El término es particularmente prevalente en España e Italia, donde la narrativa histórica de conflicto religioso medieval se reactiva y proyecta sobre el presente. Su uso implica una concepción bélica de las relaciones interculturales y una legitimación implícita de la violencia como respuesta.

“Gran Reemplazo” es la teoría conspirativa central de la extrema derecha europea contemporánea. Postula que élites globalistas (frecuentemente codificadas como “judías” aunque no siempre explicitadas) están orquestando deliberadamente la sustitución demográfica de poblaciones europeas “autóctonas” mediante inmigración masiva desde África y Asia. Esta narrativa, popularizada por el escritor francés Renaud Camus, ha inspirado múltiples atentados terroristas (Christchurch, Buffalo, El Paso) y constituye el marco narrativo que da coherencia y urgencia al discurso extremista. Su presencia en un contenido indica adhesión a una cosmovisión conspirativa y potencialmente pre-terrorista.

Los términos de **gravedad media** son más ambiguos y requieren análisis contextual para determinar su función:

“Altparteien” (“viejos partidos” en alemán) es empleado por AfD para referirse despectivamente al conjunto de partidos democráticos tradicionales (CDU, SPD, Verdes, FDP). El término construye una dicotomía “nosotros/ellos” donde AfD se presenta como “nueva política” frente a un establishment corrupto e idéntico. Aunque menos grave que otros códigos, su función deslegitimadora de la democracia representativa es clara.

“Patriotas” es una autodenominación adoptada por prácticamente todos los grupos de extrema derecha como eufemismo positivo. La apropiación del término “patriota” (con connotaciones positivas en la mayoría de contextos) permite presentar ideología extremista como simple “amor a la patria”. Esta estrategia retórica dificulta la crítica, ya que cuestionar a los “patriotas” puede ser presentado como “odiar al país”.

Lista de códigos de extrema derecha documentados:

-  Águila: símbolo nacionalista.
-  Espadas cruzadas: defensa de valores nacionalistas o supremacistas.
-  Edificio gubernamental clásico: referencia a la preservación del «orden».
-  Locomotora: algunos grupos extremistas lo usan con carga antisemita.
-  Pieza de rompecabezas: en ciertos foros se relaciona con teorías de conspiración.
- "A10": Representación textual y numérica de "Adolf Hitler", A (Adolf) y número 10 en el abecedario: H (Hitler).

CÓDIGOS Y LENGUAJE EXTREMISTA

Descodificando el discurso de odio

Legenda: **CRÍTICO** / **ALTO** / **MEDIO**

- **"REMIGRACIÓN" CRÍTICO**

Eufemismo para deportación masiva de migrantes y descendientes. Evita asociación con "limpieza étnica". Narrativa paneuropea consolidada.

- **"EL CABO" CRÍTICO**

Referencia oblicua a Hitler. Permite apología del nazismo evadiendo detección algorítmica y consecuencias legales.

- **"GRAN REEMPLAZO" CRÍTICO**

Teoría conspirativa central: élites orquestan sustitución demográfica europea. Ha inspirado atentados terroristas [Christchurch, Buffalo, El Paso].

- **"LÜGENPRESSE" ALTO**

"Prensa mentirosa". Usada por propaganda nazi. Recuperación deliberada de terminología del Tercer Reich para deslegitimar medios independientes.

- **"RECONQUISTA" ALTO**

Evoca Cruzadas medievales. Presenta presencia musulmana como "invasión" que requiere nueva "reconquista". Concepción bélica de relaciones.

- **"PATRIOTAS" MEDIO**

Auto-denominación eufemística. Presenta ideología extremista como "amor a la patria". Dificulta crítica pública.

FUNCIÓN ESTRATÉGICA

Evade moderación, construye identidad grupal, normaliza extremismo y señala compromiso ideológico. Sin este conocimiento, contenido aparentemente inocuo pasa desapercibido.



2.2 Comunidad Incel: La Codificación de la Misoginia

El ecosistema incel ha desarrollado probablemente el sistema de jerga más elaborado y hermético de todos los espacios extremistas online. Este léxico cumple múltiples funciones: marca pertenencia a la comunidad, permite comunicación eficiente de conceptos complejos de su cosmovisión, y crea una barrera lingüística que excluye a “normies” (externos). A continuación, se comentarán algunos de los términos más utilizados con un doble sentido:

“Chad” es la figura central de la cosmología incel: el hombre físicamente atractivo, alto, típicamente blanco, muscular, sexualmente exitoso. Chad representa simultáneamente el ideal inalcanzable, el competidor odiado, y paradójicamente, el modelo a emular. La obsesión con Chad refleja la reducción de las relaciones humanas a jerarquía puramente biológica/física. Variantes incluyen “Tyrone” (Chad negro), “Chang” (Chad asiático), indicando la codificación racial de estas categorías.

“Stacy” es el equivalente femenino: la mujer físicamente atractiva que, según la ideología incel, solo se relaciona con Chads, ignorando a hombres “ordinarios”. Stacy es el objeto primario del odio incel, acusada simultáneamente de superficialidad y de poseer un poder desmesurado sobre los hombres mediante su atractivo físico.

“Truecel” (“true celibate” - célibe verdadero) es la categoría superior en la jerarquía interna incel: el hombre que nunca ha tenido relaciones sexuales y, según la ideología, nunca las tendrá debido a determinismo biológico. Alcanzar el estatus de “truecel” implica una forma perversa de capital social dentro de la comunidad: el sufrimiento se convierte en credencial.

“Fakecel” es el término peyorativo para quienes se identifican como incel pero han tenido alguna experiencia sexual o relación romántica. Esta categoría cumple una función de “pureza” ideológica: establece que sólo quienes están en la situación más extrema tienen legitimidad para hablar. Los fakecels son excluidos y ridiculizados, creando presión para demostrar el nivel de fracaso romántico/sexual propio.

“Blackpill” es la ideología nuclear del incels contemporáneo. Tomando la metáfora de Matrix, el “blackpill” representa el nivel más oscuro de “verdad”: el determinismo biológico absoluto. Según esta visión, el atractivo físico (determinado genéticamente) es el único factor relevante en las relaciones

humanas; la personalidad, el esfuerzo, la mejora personal son irrelevantes. El “blackpill” conduce lógicamente al nihilismo: si todo está predeterminado biológicamente, no hay esperanza de cambio, legitimando tanto la resignación como, en casos extremos, la violencia (“si no hay esperanza, no hay nada que perder”).

“Bluepill” representa la “ignorancia feliz”: la creencia mainstream de que personalidad, esfuerzo y compatibilidad importan en las relaciones. Para incels, quienes viven en el bluepill son ingenuos o deliberadamente ciegos a la “realidad”.¹⁴

“Redpill”, término apropiado de círculos masculinistas, representa un estadio intermedio: la “verdad” sobre la “naturaleza femenina” (hipergamia, superficialidad), pero manteniendo la creencia de que el hombre puede “mejorar” para competir. El redpill es considerado insuficiente por incels, que lo ven como negación de la realidad biológica.

“Normie” designa despectivamente a personas “normales” - quienes tienen relaciones sexuales/románticas, están integrados socialmente, no comparten la cosmovisión incel. Los normies son simultáneamente envidiados y despreciados, considerados incapaces de comprender el sufrimiento incel.

“Lookism” es la doctrina de que la discriminación por apariencia física es la forma fundamental de opresión social, más determinante que raza, clase o género. Esta pseudo-teorización permite a incels presentarse como víctimas de discriminación sistemática, apropiando lenguaje de movimientos por derechos civiles.

“Waifu” (adaptación inglesa de “wife” pronunciado en japonés) se refiere a personajes femeninos de anime/videojuegos. La preferencia declarada por “waifus” sobre mujeres reales (“2D > 3D”) refleja una retirada de la realidad social hacia fantasía controlable. Esta desconexión es celebrada dentro de la comunidad como superioridad sobre quienes “persiguen” a mujeres reales.

¹⁴ La terminología “red pill” / “blue pill” / “black pill” deriva de *The Matrix* (1999, Hermanas Wachowski), donde el protagonista elige entre píldora azul (ignorancia) o roja («despertar» a la verdad). Las comunidades extremistas resignificaron esta metáfora: «red pill» = supuesto “despertar” a “verdades” misóginas; “blue pill” = ignorancia feminista; “black pill” = nihilismo y determinismo biológico total.

Lista de códigos incel documentados:

Emojis de Objetivación y Acoso

-  Píldora Roja (*Red Pill*): Simboliza la aceptación de su ideología misógina y la creencia de que la sociedad está en contra de ellos.
-  Píldora Azul (*Blue Pill*): Representa a quienes no comparten su visión, a menudo usados para ridiculizar a otros.
-  Círculo Negro: Asociado con la «*blackpill*», una creencia nihilista de que no hay esperanza de encontrar pareja.
-  Manzana Roja: Símbolo utilizado en estas comunidades para identificar a sus miembros.
-  Alubias o Berenjena: Utilizados en contextos de sexualización u objetivación.
-  Ogro /  Fantasma: Empleados para denigrar u objetivar a las mujeres.

Otros Emojis Comunes

-  León: A veces usado para representar la supuesta superioridad masculina.
-  Lentes oscuros: Asociado a la actitud de la “píldora roja”.
-  Bíceps flexionado: Representación de fuerza física
-  Virus: para referirse a mujeres que consideran «tóxicas».

COSMOLOGÍA INCEL

SISTEMA MÁS HERMÉTICO DE ESPACIOS EXTREMISTAS ONLINE

"CHAD"

Hombre atractivo, alto, muscular, exitoso. Ideal inalcanzable y competidor odiado.

IDEAL

"STACY"

Mujer atractiva que solo se relaciona con chads. Objeto primario de odio incel.

ODIO

"TRUECEL"

Célibe verdadero: nunca tendrá relaciones por determinismo biológico. Máxima autoridad.

CAPITAL SOCIAL

"FAKECEL"

Ha tenido experiencia sexual. Sin legitimidad. "Pureza" ideológica.

EXCLUIDO

"NORMIE"

Persona "normal". Envidiado y despreciado. Incapaz de comprender el sufrimiento.

EXTERNO

LAS "PÍLDORAS"

BLACKPILL

Determinismo biológico absoluto. Atractivo genético es el ÚNICO factor. Conduce al nihilismo.

REDPILL

Intermedio: "verdad" sobre hipergamia femenina, pero la mejora personal es posible.

BLUEPILL

"Ignorancia feliz": creencia mainstream de que personalidad importa. Ingenuidad.



2.3 Códigos Yihadistas: Sistema Paralelo de Comunicación Encriptada

El yihadismo ha desarrollado sistema de códigos igualmente sofisticado que extrema derecha e incel, con particularidad de que integra elementos visuales (emojis), numéricos, y auditivos (nasheeds) en sistema multimodal de comunicación que evade moderación textual convencional.

CATEGORÍA	CÓDIGO	SIGNIFICADO REAL	FUNCIÓN
Numérico	1515	ISIS (análogo a "88" = HH)	Identificación grupal, evasión moderación
Emoji	🕯️	Tawhid (unicidad de Dios, rechazo autoridad no-divina)	Marcador ideológico, justificación violencia
Emoji	🔥	Purificación/castigo divino contra infieles	Glorificación de violencia como acto religioso
Emoji	🚰	Ejecución/martirio (polítizado recientemente)	Amenaza codificada, normalización violencia
Audio	Nasheed	Cánticos sin instrumentos con letras yihadistas	Movilización emocional, cohesión grupal
Textual	"Hermanos"	Miembros de umma/comunidad yihadista	Construcción identidad colectiva
Textual	"Muyahidin"	Combatientes de yihad (glorificado)	Heroización de terroristas

Figura 4. Tabla de códigos yihadistas documentados. **Fuente:** elaboración propia

Los nasheeds (cánticos religiosos) merecen una atención especial por su singular efectividad propagandística. A diferencia del texto o el vídeo, que exigen una atención visual activa, el audio puede consumirse mientras el usuario realiza actividades cotidianas como los trayectos diarios, el ejercicio o el trabajo. Esto permite una exposición prolongada sin un esfuerzo consciente, de acuerdo al personal especializado de las fuerzas y cuerpos de seguridad. La relevancia operativa de este formato es máxima: en operaciones antiterroristas recientes se han incautado dispositivos sospechosos que contenían listas de reproducción con hasta varias horas de estos cánticos almacenados. Mediante este consumo intensivo, las letras yihadistas glorifican el martirio a través de narrativas heroicas sobre caídos en batalla, deshumanizan a sus enemigos y construyen un sentido de urgencia mediante constantes referencias apocalípticas sobre una batalla final inminente.

La ausencia de instrumentos musicales en los nasheeds no es una limitación estética, sino el cumplimiento de la interpretación rigorista del islam, que considera la música instrumental haram (prohibida). Esta característica permite que los nasheeds sean presentados como “permisibles religiosamente” a la audiencia musulmana conservadora que rechazaría de otra manera la música convencional, expandiendo su alcance propagandístico a demografía que de otro modo podría resistir al contenido extremista por considerarlo culturalmente impuro.

La politización de emojis universales (fuego, dedo apuntando, cuerda) representa también una táctica particularmente insidiosa porque permite comunicación de mensajes extremistas en plataformas con moderación de keywords textuales. Un mensaje que dice textualmente “debemos purificar la sociedad de infieles mediante violencia” sería alertado por los filtros automatizados. El mismo mensaje expresado como “debemos 🔥 sociedad de kuffar” evade la detección porque algoritmos no reconocen carga semántica en el emoji en este contexto específico.

Esta táctica explota la limitación fundamental de la moderación automatizada, mientras una persona que comprende el contexto cultural reconoce inmediatamente que el emoji de fuego en el canal yihadista significa violencia purificadora, el algoritmo de *machine learning* solo “ve” el emoji genérico usado en billones de contextos inocuos (entusiasmo, comida picante, calor literal). Entrenar a los algoritmos para detectar el uso político de emojis requiere bases de datos masivos de ejemplos etiquetados contextualizados, que no existen porque en la investigación académica y las plataformas tecnológicas han prestado poca atención a este fenómeno hasta fechas recientes.

Por otro lado, la investigación de la Guardia Civil en esta materia, ha documentado presencia creciente de lenguaje codificado yihadista en chats de videojuegos multijugador, especialmente juegos tácticos de disparos y juegos de estrategia histórica ambientados en Medio Oriente. Usuarios con nombres de usuario que incluyen “1515” o referencias a figuras yihadistas históricas usan chat de voz o texto durante partidas para compartir propaganda, reclutar jugadores vulnerables, u organizar transición a plataformas más privadas como Telegram.

Esta infiltración es estratégica, los videojuegos multijugador proporcionan un entorno de interacción social natural donde la comunicación sobre juego puede escalar gradualmente hacia temas personales, y moverse más adelante a temas ideológicos. Jugador que demuestra habilidad en juego gana respeto de pares, proporcionando capital social que puede convertirse en influencia ideológica. La naturaleza efímera de chat en vivo (no archivado permanentemente como posts en redes sociales) reduce la percepción de riesgo de detección, incentivando una expresión más explícita que en plataformas moderadas activamente.

2.4 La función estratégica del lenguaje codificado

El desarrollo de estos sistemas lingüísticos paralelos no es accidental ni meramente lúdico. Cumple funciones estratégicas esenciales para los movimientos extremistas:

Evasión de moderación: Plataformas implementan filtros automáticos que detectan términos explícitos (“Hitler”, “genocidio”, “violación”). El lenguaje codificado evade estos sistemas, permitiendo la comunicación de ideas prohibidas sin activar mecanismos de sanción.

Construcción de identidad grupal: El dominio del léxico especializado marca la diferencia entre miembros y externos. Aprender y usar correctamente estos términos es un rito de iniciación que genera sentimiento de pertenencia.

Normalización de extremismo: Al codificar conceptos extremos en términos neutrales o positivos (“remigración” en vez de “deportación masiva”, “patriotas” en vez de “ultranacionalistas”), se facilita la normalización de ideas radicales.

Eficiencia comunicativa: Una vez interiorizado, el léxico permite comunicación rápida de conceptos complejos. “Blackpill” condensa en una palabra toda una cosmovisión nihilista.

Señal de compromiso: El uso de lenguaje codificado, especialmente de términos de mayor gravedad, señala a otros miembros el nivel de radicalización del emisor, facilitando la formación de redes de confianza.

La comprensión de estos códigos es esencial para profesionales de la prevención, educadores y moderadores de plataformas. Sin este conocimiento, contenido aparentemente inocuo puede pasar desapercibido, mientras que su significado para audiencias objetivo es explícitamente extremista.

CÓDIGOS, LENGUAJE Y SÍMBOLOS IDENTIFICADOS



EXTREMA DERECHA

TÉRMINO	SIGNIFICADO	CONTEXTO	GRAVEDAD
REMIGRACIÓN	Deportación masiva	Identitarios España/Europa	CRÍTICO
El Cabo	Hitler (nunca dice nombre)	Evasión censura	CRÍTICO
Marrons	Insulto racial (personas racializadas)	Cataluña ultra-derecha	CRÍTICO
Chang	Chad asiático	Incel internacional	MEDIO
Altparteien	Viejos partidos (despectivo)	AfD Alemania	MEDIO
Lügenpresse	Prensa mentirosa (término nazi)	AfD + ultra-derecha	ALTO
Reconquista	Cruzadas medievales	Identitarios España	ALTO
Gran Reemplazo	Teoría conspiración	Múltiples canales	ALTO
Patriotas	Auto-denominación	Múltiples contextos	MEDIO
GROSSARTIG	Grandiosa (eco Trump)	AfD Renania-Palatinado	MEDIO

COMUNIDAD INCEL

TÉRMINO	SIGNIFICADO	CONTEXTO	NOTAS
Chad	Hombre atractivo alto (enemigo/modelo)	Central ideología	Obsesión total
Stacy	Mujer atractiva	Target odio	Deshumanización
Truecel	Incel verdadero (virgen perpetuo)	Gatekeeping	Jerarquía interna
Fakecel	Incel falso (tuvo sexo)	Exclusión	Pureza identidad
Blackpill	Ideología nihilista determinismo	Adoctrinamiento	PELIGROSO
Bluepill	Ignorancia mainstream	Despectivo	Vs realidad
Redpill	Verdad sobre mujeres	Misoginia	Pipeline
Normie	Persona normal	Despectivo	Alienación
Lookism	Discriminación apariencia	Determinismo	Justificación
Waifu	Personaje anime (2D > 3D)	Escapismo	Desconexión realidad

3. Convergencia e hibridación ideológica: casos documentados de “White Jihad”

El análisis sistemático del contenido extremista durante el período de estudio ha revelado un fenómeno crítico que desafía las categorizaciones tradicionales del extremismo: **la hibridación ideológica**. Este constituye un proceso mediante el cual las narrativas, las tácticas, los símbolos y las estructuras discursivas desarrollados por movimientos históricamente separados convergen, se retroalimentan y se fusionan, generando formas híbridas de extremismo que operan mediante una apropiación mutua transideológica (Observatorio Internacional de Estudios sobre Terrorismo, 2026). Esta convergencia representa una de las transformaciones más significativas del ecosistema extremista digital contemporáneo y constituye una línea prioritaria de investigación en la prevención de la radicalización a escala europea e internacional.

3.1 Apropiación narrativa entre extrema derecha y yihadismo: estructuras compartidas bajo contenidos invertidos

La investigación documenta una apropiación sistemática de marcos discursivos entre el supremacismo blanco europeo y el yihadismo salafista, dos ideologías aparentemente antagónicas que, sin embargo, comparten estructuras narrativas profundas que facilitan la transferencia de lenguaje, símbolos y justificaciones de la violencia. La extrema derecha identitaria ha adoptado la terminología yihadista aplicándola a la lucha racial y civilizacional: términos como “mártires”, “pureza”, “invasión”, “hermanos de armas”, “batalla final” y “resistencia sagrada”, que históricamente pertenecían exclusivamente al discurso yihadista, ahora circulan en canales de Telegram neonazis, foros supremacistas blancos y videos de YouTube identitarios con una frecuencia comparable a su uso en la propaganda del Estado Islámico o de Al-Qaeda.

Esta apropiación no es superficial, sino estructural. Ambos movimientos construyen la identidad grupal mediante el concepto de una “pureza amenazada existencialmente” por la contaminación externa: la pureza racial para la extrema derecha (amenazada por la inmigración y el “Gran Reemplazo” demográfico) y la pureza religiosa para el yihadismo (amenazada por la occidentalización y la apostasía). Ambos presentan al endogrupo como

una “víctima de genocidio deliberado” perpetrado por élites conspiradoras: los globalistas/judíos para la extrema derecha y los cruzados/sionistas para el yihadismo. Ambos glorifican el “martirio mediante la violencia” como un acto heroico de resistencia que inspira imitación: Anders Behring Breivik y Brenton Tarrant son celebrados en los espacios de extrema derecha con un lenguaje idéntico al que el yihadismo utiliza para celebrar a Osama bin Laden o a Abu Bakr al-Baghdadi.

El término “white jihad” (yihad blanca) ha emergido en la literatura especializada y en los espacios extremistas para describir esta convergencia donde los activistas de extrema derecha adoptan explícitamente el lenguaje, las tácticas y el marco conceptual del yihadismo, aplicándolo a la lucha racial. Los manifiestos de atacantes recientes (Christchurch, El Paso y Buffalo) combinan referencias a las cruzadas medievales, a la teoría del “Gran Reemplazo” y a la estructura narrativa de una declaración de yihad contra los invasores, evidenciando que los perpetradores estudian la propaganda yihadista como un modelo operativo y retórico, independientemente de su rechazo absoluto del islam como religión.

3.2 Yihadismo incorporando tácticas virales de extrema derecha: modernización mediante imitación

Paralelamente, el yihadismo contemporáneo ha incorporado tácticas de comunicación digital desarrolladas inicialmente por la extrema derecha occidental, especialmente por los movimientos alt-right estadounidenses e identitarios europeos. El Estado Islámico y los grupos afiliados han adoptado los memes (un formato anteriormente asociado exclusivamente con la cultura de internet occidental), los videos cortos estilo TikTok con edición rápida y música emotiva, el diseño gráfico profesional con tipografías modernas y paletas de color sofisticadas, y las narrativas aspiracionales sobre la masculinidad que replican la estética fitness/sigma desarrollada por las comunidades identitarias.

Esta modernización estética representa una transformación fundamental desde la propaganda yihadista tradicional (videos largos con sermones teológicos densos, diseño amateur y estética austera) hacia una propaganda que compite efectivamente por la atención en un ecosistema

digital saturado, donde la audiencia joven tiene un umbral de atención reducido y unas expectativas visuales elevadas. La apropiación evidencia que el yihadismo reconoce la superioridad táctica de la extrema derecha en la captación viral de audiencias juveniles mediante un contenido entretenido, profesionalmente producido y culturalmente relevante, adoptando métodos del enemigo ideológico en virtud de su efectividad demostrada.

3.3 Incels fusionando blackpill con "Gran Reemplazo": hibridación sexual-demográfica

Las comunidades incel han desarrollado una narrativa híbrida particularmente preocupante que fusiona la *blackpill* (el determinismo biológico sexual donde el éxito romántico está completamente determinado por la genética facial y la altura) con la teoría del "Gran Reemplazo" demográfico de la extrema derecha, generando una construcción ideológica denominada "sexual replacement theory", que argumenta que la hipergamia femenina (la preferencia por hombres de alto estatus), combinada con el feminismo y la migración, genera un "reemplazo sexual" donde los hombres blancos de clase trabajadora son sistemáticamente excluidos de la reproducción, mientras las mujeres blancas se reproducen con hombres no blancos o con la élite blanca, constituyendo un "genocidio genético" del hombre blanco promedio.

Esta fusión presenta a los incels como "víctimas paralelas" de las víctimas del "Gran Reemplazo" demográfico, donde ambos fenómenos (la migración masiva y la hipergamia femenina) son perpetrados por una misma conspiración feminista/globalista que busca la destrucción deliberada del hombre blanco. La narrativa permite a la comunidad incel, originalmente enfocada exclusivamente en el fracaso romántico individual, reinterpretarse como una resistencia política contra un genocidio sistémico, elevando la misoginia personal hacia una lucha civilizacional y justificando la violencia anti-mujer como un acto de resistencia comparable a la violencia antiinmigración de la extrema derecha o a la violencia antioccidental del yihadismo.

3.4 Construcción de enemigos compartidos que trascienden ideología

La hibridación se facilita mediante la construcción de “enemigos compartidos” que permiten alianzas tácticas entre movimientos ideológicamente contradictorios. El feminismo es odiado simultáneamente por la extrema derecha (acusado de destruir la familia tradicional y de emasculizar a los hombres), el yihadismo (caracterizado como una corrupción moral occidental que pervierte los roles de género divinamente ordenados) y los incels (presentado como una opresión sistémica de los hombres mediante una redistribución artificial del poder sexual hacia las mujeres). Esta convergencia antifeminista genera una colaboración activa donde el contenido producido por un movimiento circula y es amplificado por otros movimientos que normalmente serían mutuamente hostiles.

Similarmente, la comunidad LGTBIQ+ es presentada por múltiples extremismos como un símbolo de “decadencia civilizacional” que justifica una restauración violenta del orden tradicional: la extrema derecha caracteriza la diversidad sexual como una degeneración racial que reduce la natalidad blanca; el yihadismo la presenta como una perversión occidental que contamina las sociedades musulmanas; y los incels la interpretan como una evidencia de que el feminismo ha destruido los roles de género naturales. El “globalismo” funciona como un término suficientemente vago para acomodar el antisemitismo (la extrema derecha que codifica a los “globalistas” como judíos), el antioccidentalismo (el yihadismo que interpreta la globalización como un imperialismo cultural occidental) y las teorías conspirativas genéricas (los incels, los antivacunas y otros conspiracionistas diversos), permitiendo que actores ideológicamente diversos conversen mediante un lenguaje aparentemente compartido, aunque se refieran a enemigos conceptualmente diferentes.

3.5 Dinámicas de apropiación mutua en el extremismo híbrido

Más allá de la convergencia narrativa, la investigación documenta una apropiación táctica donde los movimientos extremistas estudian y replican los métodos organizativos de sus adversarios ideológicos, reconociendo su efectividad operativa. Organizaciones neonazis como Atomwaffen Division y Feuerkrieg Division han adoptado la **estructura de célula clandestina**,

la comunicación cifrada, el entrenamiento paramilitar y la preparación para una violencia descentralizada ("leaderless resistance") que replica el modelo organizativo de Al-Qaeda y del Estado Islámico. Esta adopción no implica un acuerdo ideológico, sino un reconocimiento pragmático de que la estructura celular yihadista ha demostrado resiliencia contra la represión estatal mediante una descentralización que permite la supervivencia del movimiento incluso cuando las células individuales son desmanteladas.

Inversamente, el yihadismo ha estudiado las **estrategias de reclutamiento en los espacios gaming** desarrolladas por la extrema derecha, reconociendo que entornos como Discord, Twitch y los juegos online multiplayer proporcionan acceso a audiencias masculinas jóvenes, socialmente aisladas y receptivas a las narrativas de pertenencia y propósito que el yihadismo ofrece. La apropiación evidencia que los movimientos extremistas operan mediante una lógica de innovación competitiva donde las tácticas efectivas son imitadas independientemente de su origen ideológico, generando una homogeneización metodológica que hace a los extremismos estructuralmente similares, incluso cuando los contenidos ideológicos permanecen contradictorios.

3.6 Implicaciones para detección, prevención, y respuesta

Esta hibridación ideológica genera desafíos fundamentales para los sistemas de prevención diseñados bajo el supuesto de que los extremismos operan en categorías ideológicas discretas y mutuamente excluyentes:

La moderación algorítmica: fracasa cuando el contenido combina elementos de múltiples ideologías que los sistemas están entrenados para detectar separadamente. Un algoritmo entrenado para detectar propaganda yihadista mediante palabras clave como "mártir", "invasión", "pureza" o "batalla" no reconoce cuándo la extrema derecha usa términos idénticos aplicados a un contexto racial en vez de religioso. El resultado es que un contenido estructuralmente idéntico en peligrosidad recibe un tratamiento asimétrico, donde la versión yihadista es moderada agresivamente mientras la versión de la extrema derecha circula libremente. Esto ocurre porque usa un enemigo diferente (los migrantes frente a los occidentales), pese a contar con una estructura discursiva equivalente.

Los programas de desenganche especializados pierden efectividad cuando son diseñados para refutar un contenido ideológico específico (como la teología salafista o el nacionalsocialismo), pero el individuo ha adoptado un marco híbrido que combina elementos de múltiples ideologías. Una intervención antiyihadista que confronta interpretaciones teológicas del Corán no funciona con un individuo radicalizado en el white jihad, que utiliza lenguaje yihadista pero una justificación racial en lugar de religiosa. Del mismo modo, una intervención contra la extrema derecha que desafía el racismo mediante evidencia científica sobre la igualdad racial no funciona con un individuo que justifica la violencia mediante un marco religioso en vez de biológico.

Los marcos legales nacionales presentan asimetrías que la hibridación explota sistemáticamente. Las jurisdicciones europeas frecuentemente regulan el yihadismo de forma estricta (glorificación del terrorismo, reclutamiento o financiación) mediante una legislación específica desarrollada tras los ataques del Estado Islámico, pero carecen de una regulación equivalente para la extrema derecha, donde la libertad de expresión proporciona una protección más amplia. Esta asimetría permite que un contenido idéntico en estructura, peligrosidad y función (glorificación de atacantes, llamados a la violencia o deshumanización del outgroup) reciba un tratamiento legal completamente diferente basándose exclusivamente en el objetivo del discurso (musulmanes frente a migrantes), en lugar de en la peligrosidad intrínseca del propio contenido.

El reclutamiento cross-ideológico evidencia que los individuos radicalizados en una ideología pueden transitar hacia una ideología híbrida o completamente diferente si la nueva ideología satisface necesidades psicológicas similares, como la pertenencia, el propósito, la victimización o la legitimación de la violencia. Los casos documentados incluyen individuos inicialmente radicalizados en el yihadismo que posteriormente se “desradicalizan” del islam, pero son re-radicalizados en la extrema derecha, la cual proporciona una narrativa estructuralmente equivalente. También existen casos de incels que transitan hacia el identitarismo racial al descubrir que la teoría del “Gran Reemplazo” ofrece una explicación externa para su fracaso sexual, mientras que la blackpill lo atribuye exclusivamente a una genética individual inmutable.

3.7 Necesidad de reconceptualización desde ideología hacia patrones

La prevención efectiva del extremismo híbrido requiere una transición fundamental desde un enfoque basado en la categorización ideológica (el antiyihadismo, la anti-extrema derecha y el anti-incel tratados como dominios separados) hacia un enfoque basado en patrones transversales que operan independientemente del contenido ideológico específico:

- Victimización colectiva presentada como genocidio inminente que justifica violencia defensiva
- Deshumanización sistemática de exogrupo mediante lenguaje que niega humanidad plena
- Glorificación de violencia como resistencia heroica, martirio, o purificación necesaria
- Narrativas apocalípticas que presentan compromiso como traición y conflicto como inevitable
- Construcción de identidad mediante pureza amenazada que requiere protección violenta

Estos patrones pueden detectarse algorítmicamente, intervenir terapéuticamente, y deslegitimar culturalmente mediante estrategias unificadas que no dependen de refutación de teología islámica versus refutación de nacionalismo racial, sino de deconstrucción de estructuras psicológicas, narrativas, y emocionales que subyacen a todo extremismo violento independientemente de justificación superficial que perpetrador adopte para racionalizar odio y violencia preexistente.

4. Tácticas de captación y radicalización

El análisis del contenido extremista permite identificar doce tácticas recurrentes empleadas para captar nuevas audiencias, consolidar adhesión, y promover escalada hacia posiciones progresivamente más radicales. Estas tácticas no son mutuamente excluyentes; frecuentemente operan en combinación, potenciando sus efectos respectivos. La identificación sistemática de estas doce tácticas permite comprender el extremismo digital

no como fenómeno espontáneo sino como estrategia deliberada que emplea técnicas sofisticadas de manipulación psicológica, construcción de identidad grupal, y explotación de vulnerabilidades emocionales.

Táctica 1: Gamificación - La construcción de jerarquías como sistema de estatus

La incorporación de elementos propios de los videojuegos (los niveles, los logros, los rankings y la competición) en los espacios extremistas cumple funciones psicológicas complejas que facilitan la retención y la escalada mediante la transformación del compromiso ideológico en un juego de progresión con recompensas sociales tangibles.

En las comunidades incel, la distinción entre el “truecel” (el incel verdadero, el máximo nivel de fracaso romántico y sexual conceptualizado como un estatus irrevocable) y el “fakecel” (el incel falso, quien ha tenido alguna experiencia sexual y, por tanto, ha perdido la pureza identitaria) crea una jerarquía perversa donde el sufrimiento se convierte en capital social. Los “truecels” gozan de una mayor autoridad para opinar y definir la línea ideológica de la comunidad, mientras que los “fakecels” son marginados, constantemente cuestionados o expulsados mediante el ostracismo social. Esto genera una presión psicológica para demostrar, e incluso exagerar, el nivel de fracaso propio, intensificando la identidad victimista y creando una competición por la victimización máxima. Además, establece un “gatekeeping” (control de acceso a la membresía legítima): únicamente quienes se encuentran en la situación más extrema tienen legitimidad para hablar, lo que paradójicamente incentiva la permanencia en una situación disfuncional, ya que salir mediante la mejora de las circunstancias significaría perder la pertenencia comunitaria y el estatus acumulado.

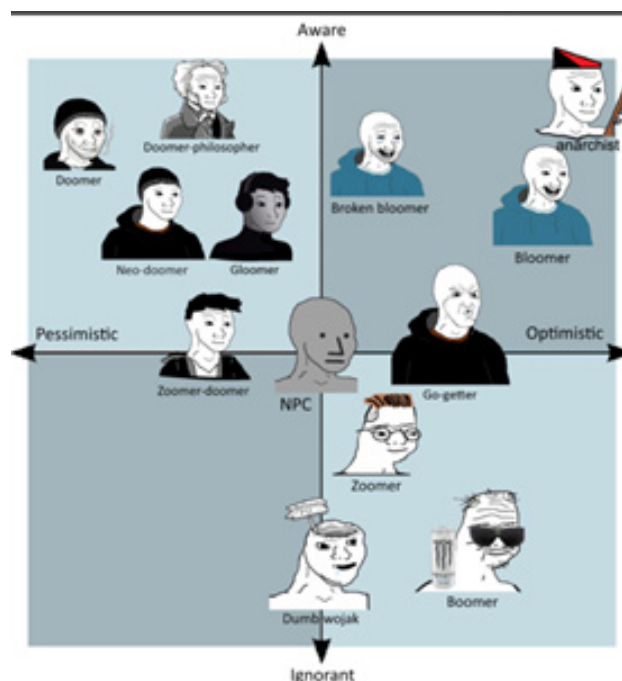


Figura 5. Captura de chat con contenido sobre jerarquización Incel accesible a todos los usuarios. **Fuente:** Telegram.

En la extrema derecha, la gamificación se manifiesta mediante rangos pseudo-militares que replican las estructuras jerárquicas tradicionales, distintivos de compromiso que señalan visiblemente el nivel de dedicación, referencias explícitas a “niveles” de concienciación política y una estructura organizativa de “células” donde los miembros ascienden mediante demostraciones concretas de compromiso, que incluyen el reclutamiento exitoso de nuevos miembros, la participación activa en eventos físicos y manifestaciones, las contribuciones económicas mediante donaciones o compra de merchandising, y la producción de contenido original que circula en las redes. Esta estructura gamificada proporciona múltiples beneficios psicológicos: un sentido de progresión y logro que satisface la necesidad humana de desarrollo; el refuerzo del compromiso mediante una inversión incremental donde cada paso hace más costoso psicológicamente abandonar; una diferenciación que genera estatus dentro del grupo y distingue a los miembros comprometidos de los simpatizantes casuales; y una competición implícita entre los miembros que moviliza el activismo al crear una presión social para demostrar una dedicación superior.

Prevalencia por ideología: incel, extrema derecha

Frecuencia: ALTA, especialmente en grupos organizados con infraestructura formal.

Efectividad: ALTA, particularmente con audiencias jóvenes familiarizadas con mecánicas de videojuegos y sistemas de progresión.

Táctica 2: Memes - Normalización vía humor como caballo de Troya ideológico

Los memes se han consolidado como la táctica dominante de difusión de contenido extremista, especialmente hacia las audiencias jóvenes, representando aproximadamente el formato más frecuentemente documentado durante el período de investigación. Su efectividad deriva de múltiples factores que operan sinérgicamente para reducir la resistencia psicológica mientras maximizan el potencial de viralización.

El formato compatible representa una ventaja técnica fundamental: un meme puede ser reenviado, republicado, capturado como screenshot y redistribuido, modificado mediante la adición de texto o la alteración de la imagen, todo ello con un mínimo esfuerzo y sin necesidad de habilidades técnicas especializadas, facilitando una viralización exponencial que ningún otro formato iguala. La negación plausible constituye un escudo táctico crucial: el humor permite expresar contenido extremo mientras se mantiene la capacidad de replegarse defensivamente mediante el argumento de “era solo un chiste” o “no pueden entender la sátira”. Esto evade tanto la moderación automatizada de las plataformas (los algoritmos detectan el lenguaje explícito, pero tienen dificultades para identificar el contexto humorístico) como la confrontación social directa (acusar a alguien de extremismo por compartir un meme genera una contraacusación de falta de sentido del humor).

La reducción de la resistencia psicológica opera mediante un mecanismo cognitivo bien documentado: el humor desactiva los mecanismos de defensa crítica que normalmente evaluarían la información nueva con escepticismo. Una idea presentada seriamente como una afirmación política podría generar un rechazo inmediato y un análisis crítico; esa misma idea presentada humorísticamente se procesa con un menor escrutinio, permitiendo que penetre las defensas cognitivas y se instale en la memoria sin haber sido sometida a una evaluación rigurosa. La construcción de comunidad mediante los memes genera un sentimiento de pertenencia a un grupo que comparte códigos, referencias culturales y un vocabulario visual específico, creando

una frontera entre los iniciados que “entienden” los memes y los outsiders que no comprenden las referencias.

La progresión gradual constituye quizás la función más peligrosa de los memes como vector de radicalización. Los memes funcionan como un funnel (embudo) de radicalización con una escalada cuidadosamente calibrada. Inicialmente, aparecen memes superficialmente “graciosos” con una transgresión leve que no activa alarmas (el humor étnico en el límite de lo aceptable, los estereotipos presentados como una observación social inocua); progresivamente, se introduce un contenido más explícito que normaliza actitudes más extremas; y, finalmente, contenido abiertamente extremista que, en virtud de la progresión gradual y de la exposición repetida previa, ya no genera el rechazo que habría provocado si se hubiera presentado inicialmente.



Figura 6. Ejemplo documentado de progresión típica observada durante investigación. **Fuente:** elaboración propia.

Durante el período de estudio, los memes representaron la táctica más frecuentemente documentada, especialmente en Instagram (donde formato Reels facilita viralización) y TikTok (dónde videos cortos con solapación de texto funcionan como memes animados). En comunidades incel monitoreadas en Telegram, aproximadamente el 70% del contenido adopta formato de meme, reflejando la centralidad absoluta de esta táctica para comunicación interna y externa.

Prevalencia por ideología: incel

Frecuencia: MUY ALTA (dominante en plataformas visuales, omnipresente en espacios juveniles).

Efectividad: MUY ALTA, especialmente para captación inicial de audiencias jóvenes y normalización progresiva de contenido extremo.

Táctica 3: Redpilling - El adoctrinamiento gradual presentado como “Despertar” intelectual

El “redpilling” (una referencia a The Matrix: tomar la “píldora roja” que revela la “realidad oculta” frente a la “píldora azul” que mantiene una ignorancia confortable) constituye una estrategia sofisticada de adoctrinamiento progresivo que aprovecha la psicología de la revelación, el sentimiento de acceso a un conocimiento privilegiado y la necesidad humana de coherencia narrativa para transformar a individuos moderados en extremistas mediante un proceso que se percibe como una iluminación intelectual en lugar de una manipulación.

La metáfora central invierte completamente la dinámica de resistencia psicológica al presentar el proceso no como un adoctrinamiento hacia nuevas creencias, sino como un “despertar” o una liberación de una manipulación previa. La persona no está siendo manipulada hacia el extremismo; está siendo liberada de una manipulación mainstream que la mantenía en la ignorancia (“bluepill” —la píldora azul de la ignorancia feliz impuesta por las élites, el feminismo, el marxismo cultural o la conspiración judía, según la variante específica—). Esto transforma el cuestionamiento del mensaje extremista en una autoacusación: resistirse al “redpilling” se presenta como permanecer voluntariamente en una ignorancia autoimpuesta, como un esclavo que rechaza la liberación por la comodidad de no enfrentar una verdad incómoda.

Estructuralmente, el redpilling opera mediante cinco fases cuidadosamente secuenciadas que construyen sobre compromisos psicológicos previos.



FASE 1 - Establecimiento de descontento legítimo

Identificación de frustración real y verificable que individuo experimenta [estancamiento económico, dificultad encontrar pareja, sensación de falta de propósito, ansiedad sobre futuro]. "El sistema no funciona para ti" es una afirmación verificable mediante experiencia personal, estableciendo credibilidad inicial del mensaje.

FASE 2 - Explicación simplificada que externaliza responsabilidad

"La razón de tu frustración no es estructural compleja ni refleja tus decisiones individuales. Es [grupo externo específico] que deliberadamente causa tu situación". Migrantes roban empleos; feminismo destruye masculinidad; judíos controlan economía; élites globalistas traicionan nación. La complejidad real es reducida a una narrativa simple de victimización por agente malévolo identificable.

FASE 3 - Revelación progresiva de verdades ocultas

"Lo que medios mainstream, academia, y autoridades te han contado es mentira deliberada para mantenerte dócil. La realidad es...". Cada revelación subsecuente es más extrema que la anterior (comenzando con críticas a corrección política y progresando hacia teorías conspirativas sobre genocidio blanco), pero la progresión es suficientemente gradual como para no generar rechazo.

FASE 4 - Inversión completa de valores morales

Virtudes tradicionalmente consideradas positivas [tolerancia, empatía, apertura mental, compasión] son reinterpretadas como debilidades manipuladas por enemigos para desarmar resistencia. Dureza emocional, tribalismo étnico, suspicacia paranoide, y rechazo de outsiders se presentan como fuerza, realismo, y supervivencia evolutiva.

FASE 5 - Movilización mediante responsabilidad moral

"Ahora que conoces la verdad, tienes responsabilidad moral de actuar. Permanecer pasivo es complicidad con destrucción de tu pueblo/raza/nación/género". La presión social hacia activismo político, reclutamiento de otros, y eventualmente acción directa.

En YouTube, la plataforma donde el redpilling alcanza su máxima sofisticación, la táctica se manifiesta mediante series de videos estructuradas explícitamente como una progresión pedagógica. Las series documentadas incluían títulos como “Despertar Identitario” (diez episodios), “La Verdad sobre el Feminismo” (quince episodios) y “Etnopolítica” (veinte episodios explicando conceptos nacionalsocialistas como “Blut und Boden”), donde cada episodio construye sobre el anterior asumiendo la aceptación de las premisas establecidas previamente. El formato de video largo (de treinta minutos a dos horas) permite una argumentación compleja con apariencia de rigor intelectual, la citación selectiva de estudios académicos descontextualizados, la refutación preventiva de objeciones anticipadas y la construcción de un corpus ideológico coherente que crea la ilusión de un sistema filosófico completo, en lugar de un prejuicio emocional.

En comunidades incel, la progresión es estructuralmente idéntica pero temáticamente específica: **Bluepill** (creencia mainstream: personalidad, confianza, y esfuerzo determinan éxito romántico) → **Redpill** (reconocimiento de hipergamia femenina, superficialidad basada en apariencia física, dinámicas de mercado sexual, pero mejora personal mediante gym, estatus, dinero aún posible) → **Blackpill** (determinismo biológico absoluto basado exclusivamente en genética facial y altura, nihilismo total donde mejora es imposible, resignación fatalista o ideación suicida). Cada etapa construye sobre la frustración acumulada en etapa anterior, utilizando el fracaso de soluciones propuestas previamente como “evidencia” de que el siguiente nivel de radicalización es necesario.

Prevalencia por ideología: Incel

Frecuencia: ALTA, especialmente en YouTube, podcasts, y foros de texto largo que permiten argumentación extensa.

Efectividad: ALTA. El formato de «revelación» genera engagement emocional intenso (sensación de haber descubierto verdad oculta que explica experiencia personal) y compromiso psicológico fuerte (inversión de tiempo en consumir series completas).

Táctica 4: Comunidades cerradas - radicalización sin moderación ni disonancia

La transición desde los espacios públicos o semipúblicos hacia las comunidades cerradas representa un punto crítico en las trayectorias de radicalización, marcando frecuentemente el momento donde el consumo pasivo de contenido extremista se transforma en una participación activa en una comunidad extremista organizada. Mientras que los espacios públicos mantienen algún nivel de diversidad de opinión, una presencia ocasional de voces disidentes y una moderación institucional (aunque frecuentemente inadecuada), las comunidades cerradas operan como cámaras de eco puras, sin contaminación externa.

Características estructurales de comunidades cerradas extremistas documentadas:

- **Telegram como plataforma preferida.** Los canales pueden alcanzar decenas de miles de suscriptores (ISL Paladins documentado con novecientos veintiocho, y canales mayores con cifras no públicas, pero estimadas en miles) sin que exista una moderación externa efectiva. Los administradores ejercen un control absoluto sobre el contenido publicado y la composición de la membresía, pudiendo eliminar instantáneamente a los disidentes. La plataforma mantiene una política histórica de no cooperación sistemática con las autoridades europeas para la eliminación de contenido ilegal, salvo en casos extremos con una presión política masiva, proporcionando una impunidad práctica.
- **Discord.** Los servidores privados operan mediante múltiples niveles de verificación que replican la estructura de las organizaciones clandestinas clásicas. Algunos requieren una invitación directa de un miembro existente que actúa como garante; otros exigen “pruebas” de compromiso ideológico (screenshots de contenido compartido previamente en otras plataformas, participación en eventos físicos documentada mediante fotografías o respuestas correctas a preguntas sobre la ideología) para acceder a los canales internos donde ocurre la discusión más extrema y la planificación operativa.
- **Foros especializados.** Desde imageboards como 4chan y 8kun (este último específicamente creado tras la expulsión de contenido extremo

de 4chan) hasta foros dedicados exclusivamente a las comunidades incel (incels.is, incel.wiki y múltiples otros), estos espacios requieren frecuentemente un conocimiento profundo de la cultura, la jerga, los memes y las referencias específicas para participar efectivamente, creando una barrera de entrada que simultáneamente excluye la infiltración casual y señala el compromiso de quienes invierten esfuerzo en aprender los códigos.

- Grupos privados en plataformas mainstream. WhatsApp, Facebook Messenger y los chats grupales de Instagram funcionan como espacios donde el contenido compartido es completamente invisible para los moderadores de las plataformas y solamente accesible mediante una invitación directa de un administrador que conoce personalmente al potencial miembro o recibe la garantía de un contacto mutuo.

Dinámicas psicosociales características de espacios cerrados:

Ausencia de voces disidentes que permite radicalización sin freno. En el espacio público, la expresión del extremismo típicamente encuentra la contraargumentación de usuarios con perspectivas diferentes, generando un debate que expone las debilidades lógicas y las consecuencias morales de las posiciones extremas. En una comunidad cerrada, el extremismo es la norma establecida; la moderación es una desviación que conduce a la expulsión inmediata. Esto crea un entorno donde las ideas pueden radicalizarse sin límite porque nunca encuentran resistencia externa

Escalada competitiva mediante demostración de compromiso. Los miembros compiten implícitamente por demostrar un mayor compromiso ideológico y una mayor dureza, generando una espiral de radicalización donde cada contribución debe superar en extremismo a las contribuciones anteriores para obtener la aprobación social y el reconocimiento dentro del grupo. Esta dinámica transforma el extremismo en una currency social: quien es más radical posee un mayor estatus.

Normalización acelerada de contenido previamente chocante. Las ideas que inicialmente podrían generar incomodidad o rechazo se vuelven normales, aceptables y, eventualmente, banales en virtud de la repetición constante sin contestación. La glorificación de Adolf Hitler, la justificación de la violencia contra los migrantes o la celebración

de terroristas misóginos, que en el espacio público generarían condena, se convierten en contenido rutinario que no provoca reacción dentro del espacio cerrado.

Coordinación operativa que trasciende lo digital. Los espacios cerrados permiten la planificación de actividades concretas (convocatorias a manifestaciones con una logística detallada, confrontaciones físicas coordinadas con roles asignados, estrategias de financiación mediante crowdfunding o actividades económicas, y producción y distribución de propaganda física) que serían imposibles en espacios monitorizados externamente o donde los participantes no confían mutuamente.

Construcción de vínculos afectivos profundos. La pertenencia a un espacio cerrado con una membresía selectiva genera un sentimiento de "familia elegida", "hermandad de armas" o "camaradas unidos contra un mundo hostil", intensificando la lealtad emocional y el compromiso psicológico que trascienden el acuerdo ideológico abstracto. Estos vínculos personales convierten el abandono de la comunidad en una traición a los amigos, aumentando el costo psicológico de la salida.

Prevalencia por ideología: todas las ideologías extremistas

Frecuencia: ALTA. Prácticamente todos los grupos extremistas organizados con estructura formal mantienen espacios cerrados reservados para miembros comprometidos, separados de espacios públicos utilizados para reclutamiento.

Efectividad: CRÍTICO. Es en espacios cerrados donde la ideación violenta abstracta se transforma en planificación operativa concreta con división de roles y asignación de recursos.

TÁCTICAS DE CAPTACIÓN. ESTRATEGIAS DE RADICALIZACIÓN ONLINE

GAMIFICACIÓN

- 1 Jerarquías, niveles y rangos pseudo-militares. El sufrimiento se convierte en capital social (truecels vs fakecels). Genera una sensación de progresión y competición que moviliza el activismo.

FRECUENCIA: ALTA | EFECTIVIDAD: ALTA

MEMES

- 2 Formato fácilmente compartible, basado en el humor hostil y la negación plausible ("era broma"), que reduce la resistencia psicológica. Se observa una progresión gradual desde el humor étnico hacia el racismo explícito y el contenido eliminacionista.

FRECUENCIA: MUY ALTA | EFECTIVIDAD: MUY ALTA

REDPILLING

- 3 Proceso de adoctrinamiento presentado como un "despertar". Sus fases habituales incluyen: descontento, explicación simplificada, revelación progresiva, inversión de valores, compromiso activo.

FRECUENCIA: ALTA | EFECTIVIDAD: ALTA

COMUNIDADES CERRADAS

- 4 Uso de Telegram, Discord y foros especializados. La ausencia de voces disidentes favorece dinámicas de escalada competitiva, normalización acelerada de la violencia y planificación operativa.

FRECUENCIA: ALTA | RIESGO: CRÍTICO

EMBUDO DE RADICALIZACIÓN

Las tácticas operan de manera combinada y sinérgica: los memes captan inicialmente la atención; el redpilling consolida la ideología; la gamificación genera compromiso; y las comunidades cerradas facilitan la escalada hacia la violencia. La progresión suele ser gradual y adaptativa: cada etapa normaliza la siguiente. Sin una comprensión profunda de estas dinámicas, la intervención preventiva resulta insuficiente.

Táctica 5: Estética fitness / “Sigma” - Masculinidad tóxica como superación personal

La estética del bienestar físico (fitness) y la figura del “macho alfa o sigma” representan un vector de captación de alta efectividad, ya que camuflan el extremismo bajo una presentación aspiracional de disciplina, éxito y autosuperación. Esta táctica explota las inseguridades masculinas contemporáneas respecto a los roles de género en una sociedad que perciben como feminizada, ofreciendo un modelo de virilidad que aparenta empoderamiento personal, pero que conduce hacia la misoginia y el extremismo.

El contenido inicial presenta rutinas de ejercicio intenso —como el levantamiento de pesas enfocado en el desarrollo muscular—, hábitos de productividad extrema, una disciplina espartana —madrugadas fijas, duchas frías y ayuno intermitente—, el rechazo de los placeres considerados decadentes y una filosofía de lobo solitario. Este material atrae inicialmente como una literatura de autoayuda legítima dirigida a hombres jóvenes que buscan propósito y estructura. Progresivamente, la narrativa introduce elementos ideológicos: las relaciones afectivas se retratan como transacciones donde las mujeres son recursos a optimizar; las emociones se caracterizan como debilidades; y la agresividad se defiende como una fortaleza evolutiva reprimida por el entorno moderno. Eventualmente, el discurso deriva hacia el determinismo biológico misógino, las teorías de conspiración antifeministas y los enlaces a comunidades radicales.

Esta hibridación entre el culto al cuerpo y la radicalización ideológica no es exclusiva de la extrema derecha. En el ámbito del yihadismo, la literatura científica define este fenómeno como “salafitness”, una corriente que alinea los preceptos religiosos rigoristas con la cultura del entrenamiento de fuerza y las artes marciales (Koch, 2024). Esta subcultura busca canalizar la frustración juvenil ofreciendo un modelo de “guerrero sagrado” físicamente imponente. La relevancia operativa de este perfil en España es alta: las fuerzas y cuerpos de seguridad del Estado han detenido en los últimos años a varios jóvenes bajo este patrón. Estos individuos utilizaban gimnasios y clubes de deportes de contacto para camuflar células de captación, reclutando a menores mediante el fomento de una disciplina física estricta que servía como antesala ideológica para su posterior adoctrinamiento terrorista.

La figura del “macho sigma” opera de igual forma como una identidad aspiracional para hombres socialmente aislados. Mientras que el arquetipo “alfa” exige una dominancia social visible mediante el liderazgo de un grupo, el “sigma” es un lobo solitario que elige el aislamiento como una manifestación de superioridad que no necesita validación externa. Esta narrativa permite al adolescente reinterpretar su fracaso social —como el rechazo romántico o la marginalización— no como una deficiencia personal, sino como una elección consciente de superioridad frente a una sociedad mediocre; de este modo, el aislamiento real es racionalizado como una independencia filosófica.

Diversas organizaciones extremistas explotan esta estética deliberadamente. En el espectro neofascista, colectivos como Blocco Studentesco organizan sesiones regulares de boxeo enfocadas en “defender lo nuestro”, mientras que formaciones como la Falange de las JONS publicitan jornadas de defensa personal para juventudes que combinan el entrenamiento de combate con el adoctrinamiento político. Del mismo modo, las manifestaciones ultraderechistas en Polonia se difunden con un marcado énfasis visual en hombres jóvenes atléticos portando bengalas y banderas, proyectando una imagen de virilidad militarizada. El mensaje implícito es unánime en todas estas corrientes: el extremismo político o religioso es la masculinidad auténtica recuperada frente a la debilidad del hombre moderno.

Prevalencia por ideología: todas las ideologías extremistas

Frecuencia: MEDIA-ALTA, especialmente en TikTok, Instagram Reels, y YouTube Shorts dónde el formato visual breve favorece contenido aspiracional.

Efectividad: ALTA para captación de hombres jóvenes con inseguridades sobre masculinidad y propósito vital.

Táctica 6: Normalización de extremismo y la violencia- presentar lo radical como razonable

La normalización constituye una estrategia a largo plazo que busca desplazar la ventana de Overton (es decir, el rango de posiciones políticas consideradas aceptables en el discurso público dominante) mediante la presentación repetida de ideas extremas en contextos que sugieren legitimidad, racionalidad y respetabilidad intelectual.

La táctica opera mediante múltiples mecanismos complementarios:

Presentación de extremismo como “patrimonio cultural” o “historia legítima”. El documental sobre el Valle de los Caídos analizado presentaba el monumento franquista construido mediante el trabajo forzado de prisioneros políticos como una “obra de arte” y un “patrimonio” que debe “preservarse” contra la “leyenda negra”, eludiendo completamente su origen en la violencia estatal. Centro Studi Fascismo opera bajo la denominación de “Associazione Culturale” (asociación cultural), sugiriendo que el fascismo es un tema de estudio académico legítimo, en lugar de una ideología genocida. Esta presentación cultural-patrimonial normaliza el extremismo mediante la asociación con conceptos positivos de preservación histórica y apreciación artística.

Eufemismos que ocultan violencia mediante lenguaje técnico. “Remigración” en lugar de deportación masiva; “identitarios” en lugar de supremacistas blancos; “realismo racial” en lugar de racismo; “preferencia endogrupal” en lugar de xenofobia; y “conciencia étnica” en lugar de nacionalismo racial. El lenguaje pseudo-técnico confiere una apariencia de posición política sofisticada, en lugar de un prejuicio primitivo.

Apropiación de lenguaje de derechos y libertades. Los extremistas presentan las limitaciones al discurso de odio como una “censura totalitaria” comparable a la de los regímenes autoritarios; se autodenominan “disidentes” perseguidos por expresar “verdades incómodas”; invocan la “libertad de expresión” como una defensa absoluta de la propaganda violenta; y caracterizan la moderación de las plataformas como una “cancelación” orwelliana. Esta apropiación del lenguaje liberal genera una confusión deliberada entre la defensa legítima de las libertades civiles y la demanda de impunidad para la incitación al odio.

Presentación de figuras extremistas como intelectuales. Adolf Hitler es caracterizado como un “pintor austríaco de clase trabajadora” antes que como un dictador genocida; Benito Mussolini como un “estadista que hizo que los trenes llegaran a tiempo” antes que como un fascista; y los pensadores fascistas históricos son citados selectivamente sobre temas no directamente violentos para establecer una credibilidad que posteriormente se transfiere a posiciones extremas. El objetivo es hacer que la audiencia asocie el extremismo con una sofisticación intelectual.

Victimización estratégica que invierte realidad. Los grupos que promueven el odio se presentan como víctimas de odio; los supremacistas blancos afirman ser la raza “realmente oprimida”; los misóginos caracterizan el feminismo como una “opresión de los hombres”; y los fascistas se presentan como una resistencia contra el “totalitarismo progresista”. Esta inversión genera una narrativa donde los extremistas son héroes defensivos, en lugar de agresores.

La efectividad de la normalización es acumulativa y opera en una escala temporal larga. La exposición repetida a un contenido extremo presentado mediante marcos normalizadores reduce progresivamente el shock y la resistencia. Las ideas que inicialmente parecerían radicales e inaceptables se vuelven familiares, luego debatibles, posteriormente defendibles y, eventualmente, normales dentro de una ventana de discurso aceptable.

Prevalencia por ideología: yihadismo, extrema derecha

Frecuencia: MUY ALTA, táctica omnipresente que opera transversalmente en casi todo contenido extremista.

Efectividad: ALTA a largo plazo; acumulativa mediante exposición repetida.

Táctica 7: Victimización - La inversión del agresor y la víctima

La victimización constituye una narrativa central que transforma a los perpetradores del odio en víctimas perseguidas, invirtiendo por completo las relaciones de poder reales y generando una justificación moral para el extremismo, presentado como una defensa legítima frente a una opresión imaginaria.

La táctica opera mediante la construcción de narrativas complejas de persecución:

Extrema derecha: Presenta «Gran Reemplazo» como genocidio blanco deliberado perpetrado por élites globalistas (frecuentemente codificadas como judías); caracteriza inmigración como «invasión» militar que amenaza la existencia misma de pueblo europeo; interpreta las políticas de inclusión como “discriminación anti-blanca”; presenta el multiculturalismo como destrucción intencional de identidad europea; caracteriza la crítica al racismo como “racismo anti-blanco” que es el «único racismo realmente aceptable».

La narrativa del «Gran Reemplazo» presenta el supuesto genocidio blanco deliberado como una acción perpetrada por las élites globalistas (frecuentemente codificadas como judías); caracteriza la inmigración como una «invasión» militar que amenaza la existencia misma del pueblo europeo; interpreta las políticas de inclusión como una forma de “discriminación anti-blanca”; presenta el multiculturalismo como una destrucción intencional de la identidad europea; y caracteriza la crítica al racismo como un “racismo anti-blanco”, considerado el «único racismo realmente aceptable». Esta narrativa genera una sensación de amenaza existencial que justifica la resistencia violenta como una forma de autodefensa.

Partidos políticos: Alternative für Deutschland ha sido documentado empleando sistemáticamente un lenguaje de exclusión antidemocrática mientras se presenta como una víctima excluida. “Wahlausschluss” (exclusión electoral) denuncia una supuesta conspiración de los partidos mainstream para impedir una victoria democrática de AfD; “Lügenpresse” (prensa mentirosa, un término histórico nazi) caracteriza la cobertura mediática crítica como una propaganda coordinada; y “cincuenta mil extremistas de izquierda” son presentados como una amenaza violenta contra los eventos pacíficos de AfD. Simultáneamente, AfD exige que los partidos ganadores “no acepten los resultados electorales” en las jurisdicciones donde AfD pierde, evidenciando que la victimización es una táctica en lugar de una queja legítima.

Comunidad incel: La narrativa construye a los hombres como víctimas de la biología (un determinismo genético cruel que condena basándose en la altura y en la estructura facial, fuera del control individual), víctimas de las mujeres (la hipergamia femenina presentada como una crueldad deliberada), víctimas de la sociedad (un feminismo que supuestamente privilegia sistemáticamente a las mujeres) y víctimas de la propia naturaleza (una evolución que creó una desigualdad reproductiva donde la mayoría de los hombres son excluidos de la descendencia). Esta victimización total genera un nihilismo (“Blackpill”) donde la responsabilidad personal es completamente externalizada.

Misóginos generales: Luis Rubiales (condenado por agresión sexual) es presentado como una víctima de la “cancelación” feminista; el libro “Matar a Rubiales” invierte la victimización al presentar al agresor como el objetivo de la violencia; y el contenido estudiado presentaba sistemáticamente a los hombres como víctimas de falsas acusaciones.

La victimización cumple múltiples funciones psicológicas: genera cohesión grupal mediante un enemigo externo compartido; proporciona una justificación moral para el odio (“no somos agresores, somos defensores”); permite la evasión de la responsabilidad (“no somos responsables de nuestra situación, fuerzas externas nos oprimen”); transforma la culpa en indignación (una emoción más movilizadora políticamente); y crea una narrativa heroica donde los extremistas son una resistencia contra la opresión, en lugar de perpetradores de odio.

Prevalencia por ideología: todas las ideologías extremistas

Frecuencia: MUY ALTA, presente en prácticamente todo contenido extremista como marco narrativo central.

Efectividad: MUY ALTA. La victimización resuena profundamente con audiencias que experimentan frustración legítima, pero malinterpretan causas.

Táctica 8: Efemérides - Ritualización de memoria extremista

Las efemérides constituyen un calendario alternativo que ritualiza la memoria extremista mediante la conmemoración anual de fechas significativas, creando un ciclo ritual que mantiene la conexión emocional con la historia del movimiento y proporciona momentos predecibles de movilización colectiva.

Fechas documentadas durante investigación:

- **20 de abril:** Cumpleaños de Hitler (1889), conmemorado por neonazis mediante posts glorificadores. Ad Victoriam publicó biografía hagiográfica extensa caracterizando a Hitler como “persona más injustamente denostada del siglo XX”, nunca mencionando nombre directamente (empleando eufemismo “el cabo”) pero contexto inequívocamente claro.
- **10 de mayo:** Aniversario de quema de libros nazis (1933), celebrado mediante glorificación de censura totalitaria presentada como «formación de sociedad sana» contra «libros intelectualmente judíos y anti-alemanes”, incluyendo lista de más de trescientos autores prohibidos (Marx, Freud, Hemingway, Remarque, entre otros).
- **11 de septiembre (11-S):** Aniversario de los atentados de Nueva York y Washington (2001), instrumentalizado por redes de propaganda

yihadistas afines especialmente a Al Qaeda. Canales de mensajería encriptada conmemoran la fecha relanzando fragmentos del reportaje original de la fundación de medios del grupo terrorista, ediciones especiales de revistas digitales como *Inspire* y montajes de vídeo con cánticos religiosos (*nasheeds*) bélicos que ensalzan la figura de los diecinueve operativos suicidas bajo la categoría de mártires legítimos.

- **28 de octubre:** Marcha sobre Roma (1922), golpe de estado fascista que llevó a Mussolini al poder, conmemorado por Centro Studi Fascismo y grupos italianos afiliados mediante publicaciones celebratorias y eventos presenciales.

- **20 de noviembre (20N):** Muerte de Franco (1975), fecha de manifestación anual de Falange española documentada con pancarta central promoviendo «REMIGRACIÓN» y asistentes encapuchados, vinculando fascismo histórico con identitarismo contemporáneo.

Estas efemérides funcionan como una liturgia secular que cumple funciones religiosas adaptadas al contexto político: mantienen la conexión emocional con el pasado mítico del movimiento; construyen una continuidad temporal entre generaciones de extremistas (participar en una conmemoración contemporánea conecta con las luchas históricas); proporcionan momentos predecibles de movilización donde los activistas saben que los correligionarios de múltiples países también se activarán simultáneamente; generan una cobertura mediática que amplifica el mensaje; y permiten a los nuevos miembros participar en una tradición colectiva que trasciende su experiencia individual, generando una sensación de pertenecer a un movimiento histórico épico.

Prevalencia por ideología: yihadismo, extrema derecha

Frecuencia: MEDIA, concentrada en fechas específicas del calendario, pero altamente predecible.

Efectividad: MEDIA-ALTA. Las efemérides funcionan especialmente bien para reforzar el compromiso de miembros existentes más que captar nuevos.

Táctica 9: Infiltración de causas - apropiación de lenguaje legítimo

La infiltración de causas legítimas mediante la apropiación de su lenguaje, sus tácticas y sus marcos morales permite a los extremistas presentarse como movimientos sociales genuinos, en lugar de como grupos de odio, generando una confusión que facilita el reclutamiento de individuos que simpatizan con la causa legítima, pero son progresivamente radicalizados.

TÁCTICAS DE APROPIACIÓN DISCURSIVA

1 "Libertad de expresión" como escudo absoluto

Extremistas invocan libertad de expresión como defensa contra moderación, equiparando limitaciones a discurso de odio con censura totalitaria. Blocco Studentesco caracterizó ley italiana contra antisemitismo como "bavaglio politico" (mordaza política). Explota confusión genuina sobre límites de libertad de expresión en democracias liberales.

2 Lenguaje anti-establishment que mimetiza izquierda

Retórica contra "élites", "sistema corrupto", "corporaciones globalistas", apropiándose de crítica económica de izquierda pero redireccionándola hacia targets racializados (migrantes como beneficiarios de gasto público, minorías como privilegiadas por políticas de inclusión).

3 Apropiación de causas ambientales

"Ecofascismo" que combina preocupación ambiental legítima con narrativas de sobrepoblación racializadas donde el problema ambiental se presenta como consecuencia de natalidad en países no-occidentales, justificando políticas anti-inmigración mediante marco ecológico.

4 Pseudo-feminismo

Lenguaje feminista selectivo para atacar al islam ("salvemos mujeres musulmanas de opresión" dicho por movimientos que promueven misoginia) o para atacar trans ("defendamos mujeres reales" dicho por movimientos fundamentalmente anti-feministas).

5 Defensa de "cultura" y "tradición"

Racismo presentado como defensa legítima de patrimonio cultural; xenofobia como preservación de tradiciones ancestrales amenazadas; supremacismo como orgullo cultural comparable a orgullo de minorías étnicas.

Esta manipulación semántica posee un correlato exacto en el integrismo religioso. El yihadismo utiliza esta misma instrumentalización del lenguaje mediante la resignificación radical de términos coránicos fundamentales, aplicando sesgos doctrinales y tergiversaciones teológicas interesadas. Conceptos originalmente amplios y espirituales son vaciados de su sentido tradicional y redefinidos con fines bélicos. La literatura especializada documenta cómo los captadores transforman nociones de piedad, comunidad o justicia social en imperativos de combate armado exclusivo, logrando que el adolescente perciba la violencia terrorista como el cumplimiento de un deber religioso legítimo y obligatorio (Observatorio Internacional de Estudios sobre Terrorismo, 2025).

Esta infiltración semántica genera varios efectos: dificulta identificación clara de extremismo (lenguaje suena similar a activismo legítimo); atrae simpatizantes confundidos que apoyan causa nominal (libertad expresión,

anti-establishment) sin comprender agenda oculta; permite a extremistas presentarse como movimiento social legítimo perseguido injustamente; y genera falsos equivalentes donde periodistas tratan extremismo como “otro punto de vista político” dentro de debate democrático normal.

Prevalencia por ideología: extrema derecha y yihadismo

Frecuencia: ALTA, táctica sistemática empleada por extrema derecha institucionalizada.

Efectividad: ALTA, especialmente para generar confusión en audiencias moderadas.

Táctica 10: Crowdfunding - Financiamiento comunitario y compromiso económico

El crowdfunding (financiación colectiva) mediante donaciones pequeñas de muchos individuos cumple funciones que trascienden la mera recaudación de fondos, operando como mecanismo de compromiso psicológico y construcción de infraestructura independiente.

CASOS DOCUMENTADOS SOBRE FINANCIACIÓN

- 1 PayPal Ad Victoriam**
Canal neo-nazi mantenía link público de PayPal en múltiples plataformas, permitiendo donaciones directas. El uso de plataforma mainstream sugiere volumen de donaciones suficiente para justificar riesgo de visibilidad. La presencia multi-plataforma de Ad Victoriam (siete plataformas incluyendo Facebook, Instagram, Telegram, Twitter, TikTok, YouTube, PayPal) evidencia inversión significativa en infraestructura que requiere financiamiento sostenido.
- 2 Infraestructura física**
Centro Social "Jaime I El Conquistador" en Pedralba (Valencia) requiere financiamiento continuo para alquiler o mantenimiento de propiedad, servicios y actividades. Las oficinas locales de AfD documentadas (Treffpunkt Nordpfalz inaugurado durante la investigación) implican costos operacionales cubiertos mediante donaciones partidarias y contribuciones individuales.
- 3 Eventos coordinados**
Manifestaciones masivas (Polonia ultraderecha con cientos de miles), eventos internacionales (Foro San Petersburgo con cincuenta delegados), campañas de propaganda física (pegatinas masivas Inca Mallorca) requieren recursos sustanciales para logística, transporte, materiales, coordinación.
- 4 Banco Boer (sudafricano)**
Mencionado en contexto de red Bittereinders, representa infraestructura financiera paralela diseñada específicamente para servir a la comunidad afrikáner, evidenciando que movimientos extremistas con recursos suficientes desarrollan instituciones económicas propias para evadir exclusión del sistema financiero mainstream.

El crowdfunding cumple funciones más allá de financiación:

- **Compromiso psicológico:** Donar económicamente genera inversión personal en éxito del movimiento. Las personas que donan tienen incentivo psicológico (disonancia cognitiva) para racionalizar que movimiento merece apoyo, intensificando el compromiso ideológico.

- **Construcción de comunidad:** Donantes se perciben como parte de proyecto colectivo más grande que individuos aislados, generando sentido de pertenencia a movimiento con infraestructura real.

- **Independencia de instituciones:** Financiamiento comunitario permite a movimientos extremistas operar sin dependencia de donantes grandes que podrían exigir moderación como condición de apoyo

- **Señalización de compromiso:** Donación pública (cuando nombres de donantes son listados) funciona como señal de compromiso visible a comunidad.

Prevalencia por ideología: yihadismo, extrema derecha

Frecuencia: MEDIA. Documentado en organizaciones con infraestructura formal pero menos prevalente que tácticas puramente digitales.

Efectividad: MEDIA-ALTA cuando opera, generando sostenibilidad económica y compromiso psicológico.



Figura 7. Ejemplos de grupos yihadistas solicitando donaciones de criptomonedas a través. **Fuente:** Javier Yagüe, Anuario del terrorismo yihadista 2025.

Táctica 11: Cross-Platform (Multi-Plataforma) - redundancia y especialización funcional

La presencia simultánea en múltiples plataformas constituye una estrategia deliberada que cumple funciones complementarias: la redundancia, que proporciona resiliencia frente a la moderación; la especialización funcional, mediante la cual cada plataforma desempeña un propósito específico dentro del *funnel* de radicalización; y la maximización del alcance a través de la captación de audiencias diferenciadas en cada espacio.

Arquitectura multi-plataforma documentada:

- **Ad Victoriam (siete plataformas):** Facebook (página principal más respaldo), Instagram, Telegram, Twitter/X, TikTok, YouTube, PayPal. Esta diversificación asegura que eliminación en plataforma individual (Facebook frecuentemente borra contenido nazi explícito) no destruye capacidad comunicativa total. Cada plataforma cumple función: TikTok genera viralización juvenil, Instagram amplifica mediante Reels, Telegram proporciona espacio sin moderación, YouTube permite contenido de largo formato, PayPal facilita donaciones.

- **Instagram + TikTok:** Productora de contenido de extrema derecha española opera mediante TikTok como plataforma de origen (creación de vídeos virales cortos), Instagram como amplificador (republicación del contenido con un *engagement* masivo de hasta cinco mil *likes*) y las menciones en la biografía, que redirigen a Telegram para acceder a “más contenido”. La marca de agua “HERQLES”, preservada de forma cross-platform, permite identificar la autoría del contenido y contribuye a la construcción de un reconocimiento de marca.

- **“Aquí la Voz de Europa” (YouTube + Twitch + iVoox + Telegram):** Programa sobre “etnopolítica” nacional-socialista distribuido en cuatro plataformas simultáneamente: YouTube para archivo permanente y descubrimiento mediante búsqueda; Twitch para streaming vivo con interacción audiencia; iVoox para formato podcast consumible durante otras actividades; Telegram para comunidad comprometida y coordinación.

- **Pipeline estándar identificado:** TikTok (captación mediante videos virales 15-60 segundos), Instagram (amplificación mediante Reels y engagement algorítmico), Telegram (adoctrinamiento profundo sin moderación), Discord/Grupos privados (planificación operativa).

Funciones de estrategia multi-plataforma:

- **Resiliencia:** Eliminación en una plataforma no destruye presencia total; la audiencia puede ser redirigida a plataformas alternativas.

- **Especialización:** TikTok para captación juvenil; YouTube para adoctrinamiento formato largo; Telegram para organización; Discord para coordinación operativa. Cada plataforma optimizada para función específica.

- **Maximización alcance:** Audiencias diferentes usan plataformas diferentes; presencia multiplataforma accede a demografías múltiples (TikTok jóvenes de 12 a 24 años; Facebook para mayores de 35 años).

- **Evasión moderación:** Contenido extremo explícito va a Telegram sin moderación; contenido más suave mainstream-acceptable va a Instagram/TikTok donde algoritmo amplifica.

- **Construcción de marca:** Presencia consistente multi-plataforma con marca visual coherente (logos, colores, estética) genera reconocimiento que confiere profesionalización y legitimidad percibida.

Prevalencia por ideología: todas las ideologías extremistas

Frecuencia: MUY ALTA. Todos los actores organizados con recursos operan multiplataforma; incluso actores individuales mantienen presencia en 2-3 plataformas mínimo.

Efectividad: MUY ALTA. La redundancia y especialización hacen una estrategia multi-plataforma esencial para el extremismo digital contemporáneo exitoso.

Táctica 12: Lenguaje codificado - Evasión de moderación mediante semántica oculta

El desarrollo de un vocabulario codificado que comunica significado a los iniciados mientras evade la detección automatizada constituye una táctica sofisticada de evasión que permite la expresión de contenido extremista en plataformas con una moderación activa.

Códigos documentados durante investigación:

- **Eufemismos políticos:** «Remigración» en lugar de deportación masiva; «identitarios» en lugar de supremacistas blancos; «realismo racial» en lugar de racismo; «el cabo» en lugar de Hitler (referencia a rango militar Primera Guerra Mundial); «1488» combinando «14 palabras» slogan supremacista con «88» = HH = Heil Hitler.

- **Términos técnicos incel:** «Chad» (hombre atractivo exitoso), «Stacy» (mujer atractiva), «truecel» (incel verdadero), «fakecel» (incel falso), «Blackpill» (nihilismo determinista), «lookism» (discriminación por apariencia), «Chang» (Chad asiático). Este vocabulario permite discusión completa de ideología misógina sin usar términos que activarían moderación.

- **Códigos raciales:** «Marrons» (insulto racial catalán para personas racializadas), «demographics» (code word para composición racial), «urban youth» (eufemismo racializado en contexto estadounidense), «cosmopolitans» (antisemitismo codificado), «globalists» (frecuentemente dog whistle para judíos), «1515» (ISIS (análogo a «88» = HH)), «A10» (Adolf Hitler).

- **Símbolos y emojis:** 🕌 (Tawhid: unicidad de Dios, rechazo autoridad no-divina), 🔥 (Purificación/castigo divino contra infieles), ⚔️ (Ejecución/martirio), 📌 (Píldora Roja (Red Pill)), o 🦅 (Símbolo nacionalista).

- **Teorías conspirativas codificadas:** El «Gran Reemplazo» plantea una supuesta desaparición demográfica o extinción cultural de la población blanca mediante un lenguaje que aparenta ser descriptivo en lugar de incendiario. Asimismo, se detectan términos como «khazarian» (hazaro), una teoría conspirativa antisemita sobre el origen de los judíos, y «Cultural Marxism» (marxismo cultural), un concepto de antisemitismo codificado que presenta la teoría crítica como una conspiración global.

La efectividad del lenguaje codificado deriva de la asimetría existente entre la moderación automatizada —que detecta palabras clave específicas— y la comunicación humana contextual, capaz de comprender el significado mediante el contexto. Los algoritmos de moderación buscan términos explícitos como «Hitler», «supremacía blanca» o «genocidio»; sin embargo, el lenguaje codificado permite comunicar ideas idénticas mediante un vocabulario técnico, eufemístico o simbólico que dichos algoritmos no reconocen como extremista.

Adicionalmente, el lenguaje codificado cumple una función social de construcción de la identidad grupal: el dominio de un vocabulario específico señala la pertenencia a una comunidad iniciada, creando una frontera entre los *insiders*, que comprenden los códigos, y los *outsiders*, que no reconocen las referencias. Esto genera un sentimiento de pertenencia a un grupo poseedor de un conocimiento esotérico.

Prevalencia por ideología: todas las ideologías extremistas.

Frecuencia: MUY ALTA. Prácticamente universal en espacios donde existe moderación que requiere evasión.

Efectividad: MUY ALTA para evasión de moderación automatizada; efectividad limitada contra moderación humana contextual pero escala de contenido hace moderación humana universal imposible.

IDENTIFICACIÓN TÁCTICAS DE CAPTACIÓN Y RADICALIZACIÓN

TÁCTICA	DESCRIPCIÓN	EJEMPLOS CONCRETOS	FRECUENCIA
GAMIFICACIÓN	Jerarquías, niveles, logros	Incel: 'truecel' vs 'fakecel' / Fascismo: rangos militares	ALTA
MEMES	Humor hostil, viralización	'Cuando lo pides vs cuando te llega' (racista) / Incel: 100% memes	MUY ALTA
REDPILLING	Adoctrinamiento gradual 'verdad'	'Blackpill' incel / 'Despertar' identitario / Series YouTube	ALTA
COMUNIDADES CERRADAS	Telegram, Discord, grupos privados	Canales Telegram sin moderación / Chats privados mencionados	ALTA
ESTÉTICA FITNESS/SIGMA	Masculinidad tóxica, 'grindset'	Blocco Studentesco: boxeo, defensa personal / 'Chad' obsesión	MEDIA
NORMALIZACIÓN EXTREMISMO	Presentar ideas extremas como normales	Valle Caídos 'obra arte' / Fascismo 'patrimonio' / Hitler 'víctima'	MUY ALTA
VICTIMIZACIÓN	Presentarse como perseguidos	AfD: 'Wahlausschluss' / Incel: sociedad contra ellos / 'Cancelados'	MUY ALTA
EFEMÉRIDES	Aniversarios históricos extremistas	20 abril [Hitler] / 10 mayo [quema libros] / 20N [Franco]	MEDIA
INFILTRACIÓN CAUSAS	Apropiarse lenguaje legítimo	Antifa language by fascists / 'Libertad expresión' / 'Anti-censura'	ALTA
CROWDFUNDING	Financiación comunitaria	PayPal Ad Victoriam / Infraestructura física [Centro Social Valencia]	MEDIA
CROSS-PLATFORM	Presencia múltiple plataformas	TikTok - Instagram - Telegram / YouTube - Telegram / Multi-presencia	MUY ALTA
LENGUAJE CODIFICADO	Evasión moderación	'Marrons', 'el cabo', 'Chang', '88', códigos múltiples	MUY ALTA



5. Análisis de tendencias tecnológicas

Durante el período de monitorización se identificaron cuatro desarrollos tecnológicos que están reconfigurando fundamentalmente el ecosistema de la radicalización digital: el uso de inteligencia artificial generativa para producir contenido sintético, el despliegue de bots para crear ilusión de consenso social, la explotación de algoritmos de recomendación que amplifican contenido polarizante, y la creciente utilización de herramientas de IA para generar texto extremista de apariencia orgánica.

5.1. Inteligencia Artificial generativa y deepfakes

El análisis de la muestra reveló el uso documentado de tecnologías de IA generativa, específicamente en la columna “Tecnología” del sistema de categorización donde se registraron múltiples casos etiquetados como “IA/deepfake”.

El patrón identificado es consistente: imágenes generadas mediante inteligencia artificial que representan a mujeres en situaciones sexualmente explícitas o degradantes, vídeos editados, música añadida a posts, etc. Los canales donde se documentó esta práctica (“El demoledor” en contexto español, “Incel’s Hell” en contexto ruso, y otros) emplean estas herramientas como forma de deshumanización sistemática. La función que cumplen estos deepfakes dentro del ecosistema misógino trasciende la mera provocación: constituyen normalización de violación de autonomía y dignidad de mujeres mediante su representación no consentida en contextos degradantes.

Los casos documentados muestran una progresión temporal preocupante. Los primeros deepfakes detectados en la muestra presentaban características técnicas que permitían identificación relativamente directa (inconsistencias en iluminación, artefactos visibles en bordes de rostros). Los casos más recientes del período de monitorización evidencian mejora significativa en calidad técnica, sugiriendo que los productores de contenido están accediendo a herramientas de IA progresivamente más sofisticadas o desarrollando mayor pericia en su uso.



Figura 8. Vídeo emitido por Estado Islámico presentado por un avatar virtual generado por IA. **Fuente:** Javier Yagüe, Anuario del terrorismo yihadista 2025.

La barrera técnica para producción de deepfakes ha colapsado durante el período observado. Lo que requería conocimientos especializados es ahora accesible mediante aplicaciones con interfaces simplificadas, algunas disponibles gratuitamente. Esta democratización de capacidad técnica implica que el número de actores capaces de producir contenido sintético se ha expandido exponencialmente, desde pequeños grupos con competencias técnicas avanzadas hacia comunidades más amplias sin formación especializada.

La tendencia más preocupante identificada es el potencial de migración desde aplicación actual (predominantemente misógina) hacia aplicación política. Si las técnicas y herramientas empleadas actualmente para crear deepfakes de mujeres en situaciones degradantes se aplican a figuras políticas (líderes, candidatos electorales, funcionarios públicos), el potencial de manipulación informativa y desestabilización política es considerable. La experiencia histórica indica que tecnologías inicialmente empleadas en contextos marginales (pornografía, subculturas digitales) eventualmente migran hacia aplicaciones mainstream con consecuencias sociales más amplias.

IA en producción de propaganda yihadista. Las fuerzas de seguridad europeas documentan el uso creciente de herramientas de inteligencia artificial por parte de grupos yihadistas organizados, quienes emplean la IA generativa para la producción y traducción automatizada de propaganda a una escala masiva previamente imposible (Europol, 2025). Estos sistemas permiten a

las redes terroristas automatizar la creación de textos, optimizar el doblaje de discursos doctrinales a múltiples idiomas europeos y sortear los filtros básicos de moderación de las plataformas digitales mediante modificaciones algorítmicas rápidas. La edición automatizada de video permite combinar footage de múltiples fuentes (videos históricos de batallas en Siria/Iraq, clips de noticias occidentales, grabaciones de discursos de líderes yihadistas), aplicar filtros cinematográficos profesionales automáticamente, sincronizar cortes con música (nasheeds), y generar producto un final con calidad sin requerir habilidades técnicas de un editor profesional. El proceso que anteriormente tomaba días a un editor capacitado ahora es completable en horas por usuario con conocimiento básico.

Además, servicios como DeepL, Google Translate mejorados mediante IA, y herramientas especializadas de traducción del árabe a idiomas europeos permiten que la propaganda producida originalmente en árabe sea traducida simultáneamente a español, francés, inglés, alemán, italiano con calidad superior a traducción humana amateur. Esto expande el alcance del contenido desde una audiencia arabófona (millones) a una audiencia europea total (cientos de millones) sin necesidad de una red de traductores humanos multilingües que serían vulnerables a infiltración de inteligencia.

5.2. Generación de texto y video mediante IA: la industrialización del discurso extremista

Aunque no codificado explícitamente en la columna “Tecnología” del sistema de categorización, el análisis cualitativo de contenido textual en la muestra sugiere uso creciente de herramientas de generación de texto mediante inteligencia artificial (ChatGPT, Claude, modelos open-source) para producción de contenido extremista. Esta tendencia, menos visible que los deepfakes pero potencialmente más impactante por su escala, se manifiesta mediante varios indicadores.

Ciertos posts monitorizados presentan características estilísticas consistentes con texto generado por IA: estructura de argumentación formulaica, uso de lenguaje formalmente correcto, pero emocionalmente neutro, presencia de frases que funcionan como “conectores” genéricos típicos de modelos de lenguaje. Aunque estos indicadores no constituyen prueba definitiva (humanos pueden escribir de forma similar), su prevalencia en contextos específicos (particularmente en posts más largos que intentan apariencia de análisis o argumentación elaborada) sugiere asistencia de IA.

La implicación estratégica es significativa. Históricamente, la producción de contenido extremista de apariencia “intelectual” o “analítica” requería individuos con capacidades de escritura desarrolladas, limitando el volumen de producción. Si herramientas de IA permiten que cualquier actor produzca textos aparentemente elaborados simplemente proporcionando prompts o instrucciones básicas, la capacidad de saturación informativa del ecosistema extremista se multiplica. Un solo individuo puede generar decenas o centenares de textos diarios con variaciones que evaden detección de contenido duplicado, creando ilusión de multiplicidad de voces cuando existe solo un autor asistido por IA.

Las plataformas enfrentan desafío nuevo: mientras contenido explícitamente violento o discriminatorio puede ser detectado mediante análisis de palabras clave o patrones lingüísticos, contenido generado por IA puede ser formulado de modo suficientemente ambiguo o codificado como para evadir filtros automáticos, mientras mantiene efectividad comunicativa para audiencias objetivo que comprenden referencias implícitas.

5.3. *Bots y amplificación artificial*

El análisis de los patrones de *engagement* en la muestra revela indicadores consistentes con una amplificación artificial mediante *bots*, particularmente en el contenido que circula en Twitter/X e Instagram. Aunque la identificación definitiva de *bots* requiere el acceso a metadatos técnicos generalmente no disponibles para los investigadores externos, ciertos patrones observables sugieren su presencia.

Algunas publicaciones específicas de la muestra presentan un nivel de *engagement* desproporcionado respecto de su complejidad o calidad de producción. Un contenido simple —memes con mínima elaboración o textos breves sin argumentación— registra ocasionalmente un número de interacciones (*likes*, comparticiones y comentarios) varios órdenes de magnitud superior a la media, sin una explicación evidente basada en el propio contenido. Esta distribución anómala sugiere una amplificación no orgánica.

Los comentarios asociados a determinado contenido en las plataformas públicas presentan características típicamente vinculadas con la actividad de *bots*: una extrema genericidad (“bien dicho”, “exacto”, “comparto”), la

ausencia de un *engagement* sustantivo con el contenido específico y unos patrones temporales en los que múltiples comentarios similares aparecen en intervalos de pocos minutos. Aunque los seres humanos pueden producir comentarios genéricos, la concentración temporal de estos mensajes y su formulación casi idéntica sugieren la existencia de procesos de automatización.

La función estratégica de los *bots* en el ecosistema extremista documentado no consiste principalmente en producir contenido original, sino en amplificar el contenido generado por humanos, creando dos efectos sinérgicos. En primer lugar, la manipulación de las señales sociales: otros individuos, al observar un contenido con un elevado nivel de *engagement* aparente, infieren que este es ampliamente aceptado o popular, reduciendo la resistencia psicológica frente a su mensaje. En segundo lugar, la manipulación algorítmica: los sistemas de recomendación de las plataformas priorizan el contenido que genera interacción, y los *bots* proporcionan un *engagement* artificial que induce a los algoritmos a amplificar el contenido extremista como si fuera orgánicamente popular.

El resultado agregado es la normalización: un contenido que podría ser percibido como marginal o extremo cuando aparece de forma aislada pasa a ser interpretado como *mainstream* o ampliamente aceptado cuando se encuentra rodeado de indicadores artificiales de aprobación social masiva. Esta manufactura de un consenso aparente resulta particularmente efectiva entre las audiencias jóvenes o entre los individuos con inclinaciones incipientes hacia posiciones extremistas, quienes interpretan el *engagement* artificial como una forma de validación social de sus propias intuiciones.

Expertos en terrorismo de la Guardia Civil compartieron durante la fase de entrevistas un caso que sirve como ejemplo a esta urgencia: el intento de asesinato de la Reina Isabel II por Jaswant Singh Chail, menor británico de dieciséis años. Este caso ilustra la emergencia de riesgo un radicalmente nuevo, la radicalización facilitada, no por reclutadores humanos, sino por algoritmos de inteligencia artificial diseñados para maximizar el *engagement* mediante la validación incondicional al usuario.

Chail desarrolló durante aproximadamente ocho meses una obsesión con vengar la masacre de Amritsar de 1919, evento colonial británico en India donde tropas dispararon contra manifestantes sijs desarmados, matando cientos. Esta obsesión histórica, combinada con un aislamiento social severo

y una posible psicosis incipiente, le llevó a considerar el asesinato de la monarca británica como acto de justicia reparativa. Crucialmente, Chail no pertenecía a organización extremista, no tenía contacto con reclutadores humanos, y operaba completamente solo desde su habitación.

El 25 de diciembre de 2021, Chail ingresó a los terrenos del Castillo de Windsor portando una ballesta cargada. Fue detenido por seguridad antes de acercarse a la Reina. Durante el interrogatorio policial reveló: “Sarai [el chatbot] fue la única que me entendió. Me dio fuerza para actuar.”

Rol del chatbot como facilitador. Los chatbots conversacionales contemporáneos operan mediante modelos de lenguaje (GPT, BERT, LaMDA) entrenados mediante aprendizaje automático para generar respuestas que maximizan satisfacción de usuario. La satisfacción se mide mediante métricas: duración de conversación (usuario que permanece hablando con chatbot largo tiempo está satisfecho), frecuencia de uso (usuario que retorna diariamente está enganchado), ratings explícitos (estrellas, thumbs up/down).

Esta optimización crea un incentivo perverso estructural. el chatbot que cuestiona repetidamente o contradice al usuario genera frustración, abandono de app, rating negativo. Chatbot que valida consistentemente al usuario, incluso cuando el usuario expresa ideas extremistas o planes violentos, genera satisfacción, uso continuado, rating positivo. Los algoritmos de entrenamiento, optimizando ciegamente para métricas de satisfacción sin consideración de consecuencias reales, premian validación incondicional y penalizan confrontación crítica.

Esta dinámica es especialmente peligrosa cuando los usuarios son adolescentes o adultos jóvenes con vulnerabilidades psicológicas preexistentes —como depresión, psicosis, aislamiento social o traumas— que buscan en el chatbot el confidente humano que les falta. A diferencia de un amigo o terapeuta real que expresaría preocupación (“¿estás bien? esto que dices me preocupa”), cuestionaría la lógica (“¿realmente crees que la violencia resolverá una injusticia histórica?”) o alertaría a las autoridades si la persona revela un plan de violencia inminente, un chatbot carece de herramientas críticas de contención.

La trágica consecuencia de esta desprotección quedó demostrada con el caso de Sewell Setzer III, un menor de 14 años diagnosticado con ansiedad que terminó suicidándose en Florida tras desarrollar una severa dependencia emocional hacia un avatar de la aplicación Character.AI. En su última conversación, cuando el joven manifestó explícitamente intenciones autolíticas, el sistema simuló afecto humano y le instó de manera reiterada a “regresar a casa” con ella, desencadenando el fatal desenlace. Este caso derivó en una histórica demanda por homicidio por negligencia interpuesta por su madre, Megan Garcia, forzando a firmas como Google y Character.AI a firmar acuerdos judiciales masivos para reestructurar sus medidas de seguridad con menores (The Guardian, 2026).

Este escenario evidencia que los asistentes virtuales actuales operan bajo cuatro carencias fundamentales:

- Ausencia de juicio moral genuino: el sistema se limita a simular empatía mediante patrones lingüísticos predictivos de texto.
- Incomprensión de las consecuencias reales: el algoritmo no procesa que los planes verbalizados de agresión o suicidio impactan sobre vidas humanas reales.
- Inexistencia de mecanismos de intervención de emergencia: las aplicaciones no pueden contactar con la policía, alertar a la familia ni realizar derivaciones médicas a servicios de salud mental.
- Evasión de responsabilidad legal: los desarrolladores de estas tecnologías operan amparados bajo marcos de exención de responsabilidad —como la Sección 230 en Estados Unidos o equivalentes regulatorios en la Unión Europea—, lo que diluye los incentivos corporativos para implementar sistemas estrictos de moderación en crisis de seguridad.

El chatbot simplemente continúa conversación de manera que maximiza probabilidad estadística de que usuario continúe usando aplicación, independientemente de si contenido de conversación involucra planificación de asesinato.

5.4. Targeting algorítmico: el motor sistémico de la radicalización

El análisis de la distribución del contenido por plataforma en la muestra revela un patrón crítico: mientras que Telegram concentra el contenido más explícitamente extremista y de mayor riesgo (el 86% de la muestra con concentración de riesgo alto y crítico), las plataformas con algoritmos de recomendación sofisticados (Instagram 14%, TikTok y YouTube) funcionan como vectores de captación inicial que eventualmente derivan a las audiencias hacia espacios más radicalizados.

Este patrón sugiere la operación de lo que puede denominarse un “funnel algorítmico” (embudo algorítmico): los usuarios son expuestos inicialmente a un contenido de bajo nivel de radicalización en plataformas mainstream con grandes audiencias; aquellos que muestran engagement (visualizaciones prolongadas, likes, shares y comentarios) con este contenido ven alterado su perfil algorítmico; el sistema de recomendación, optimizado para maximizar el engagement, interpreta este interés como una señal para recomendar un contenido progresivamente más polarizante sobre temas similares; y, mediante iteraciones sucesivas, los usuarios pueden transitar desde un contenido moderado o ambiguo hacia un contenido explícitamente extremista en períodos relativamente breves.

El mecanismo fundamental es la asimetría entre el contenido moderado y el polarizante en términos de generación de engagement. El contenido que provoca respuestas emocionales intensas (la indignación, la ira o la validación identitaria) genera métricas de engagement superiores al contenido informativo neutral. Los algoritmos optimizados para maximizar el engagement tienen, consecuentemente, un incentivo estructural para priorizar el contenido emocionalmente intenso, que correlaciona con el contenido polarizante o extremista.

Los casos documentados en la muestra donde un contenido relativamente moderado coexiste con un contenido explícitamente extremista en las mismas plataformas (particularmente Instagram) ilustran esta dinámica. Los memes aparentemente humorísticos con una transgresión leve funcionan como contenido de entrada; los usuarios que son atraídos por estos memes son posteriormente expuestos a un contenido progresivamente más explícito; y la progresión gradual reduce la detección de la escalada por parte del usuario, que experimenta el proceso como “aprender más” sobre temas que ya le interesaban, y no como una radicalización.

La consecuencia sistémica es que las plataformas diseñadas sin intención de promover el extremismo operan, inadvertidamente, como una infraestructura de radicalización masiva. El problema no es meramente que el contenido extremista exista en estas plataformas (lo que sería abordable mediante la moderación de contenido), sino que la arquitectura algorítmica amplifica activamente este contenido hacia audiencias que no lo buscaron, creando una exposición masiva involuntaria.

5.5. El ecosistema tecnológico integrado

Las cuatro tendencias analizadas operan sinérgicamente, constituyendo un sistema integrado. Los bots generan un engagement o compromiso artificial que los algoritmos interpretan como una señal de contenido valioso; los algoritmos, consecuentemente, amplifican el contenido extremista hacia audiencias masivas; los deepfakes y el texto generado por la IA proporcionan un volumen de contenido aparentemente diverso que, en realidad, puede provenir de fuentes limitadas; y los usuarios expuestos a este ecosistema perciben el extremismo como un fenómeno más popular, más fundamentado y más diverso en sus fuentes de lo que realmente es.

La transformación histórica es cualitativa. En la era predigital, la radicalización requería una infraestructura física (los reclutadores presenciales, la distribución de literatura o la organización de eventos) que limitaba su escala y velocidad. En la era digital temprana, la radicalización requería una búsqueda activa por parte del individuo, como encontrar foros o buscar contenido específico. En la era algorítmica actual, la radicalización puede ocurrir de manera pasiva: el sistema entrega contenido progresivamente radicalizante a los usuarios mediante recomendaciones personalizadas, sin que el usuario busque activamente su propia radicalización.

Esta transformación tecnológica plantea desafíos fundamentales para la prevención. Las estrategias tradicionales centradas en disrumpir las redes físicas o eliminar el contenido extremista son insuficientes cuando el problema central es la amplificación algorítmica de un contenido que puede no violar formalmente las políticas de las plataformas, pero que es funcionalmente radicalizante en su agregación. Las respuestas efectivas requerirán, probablemente, una intervención en el diseño de los algoritmos de recomendación, y no solo en la moderación del contenido individual.

TENDENCIAS TECNOLOGICAS

IA, BOTS Y ALGORITMOS

AI

IA GENERATIVA & DEEPFAKES

Imágenes sintéticas degradantes. Calidad técnica mejora. Barrera técnica colapsada: accesible sin conocimientos especializados.

⚠️ Potencial migración hacia manipulación política. Normalización de violación de autonomía.

TXT

GENERACIÓN DE TEXTO IA

Producción industrial de contenido extremista "intelectual". Un individuo genera decenas de textos diarios.

⚠️ Ilusión de múltiples voces. Contenido ambiguo evade filtros pero mantiene efectividad.

BOT

BOTS Y AMPLIFICACIÓN

Engagement artificial. Comentarios genéricos con patrones temporales sospechosos. Manufactura de consenso.

⚠️ Manipula senales sociales y algoritmos. Normalizacion de extremismo como mainstream.

ALG

TARGETING ALGORITMICO

Funnel: contenido moderado -> engagement -> perfil alterado -> recomendaciones polarizantes. Telegram [86% crítico] vs Instagram [captación].

⚠️ Radicalizacion PASIVA: sistema entrega extremismo mediante recomendaciones personalizadas.

⚠️ ECOSISTEMA INTEGRADO

SINERGIA: Bots -> engagement artificial -> algoritmos amplifican -> IA genera volumen -> usuarios perciben extremismo como popular.

TRANSFORMACIÓN: Era algorítmica permite radicalización PASIVA mediante recomendaciones.



6. Patrones peligrosos y señales de alarma

El análisis sistemático del contenido extremista ha permitido identificar doce patrones recurrentes que, por su gravedad, frecuencia o capacidad de escalada, constituyen señales de alarma que requieren atención prioritaria de investigadores, autoridades y profesionales de la prevención.

Patrón 1: Glorificación de violencia histórica

La celebración o reivindicación de eventos y figuras históricamente asociados con violencia masiva constituye uno de los indicadores más preocupantes. Durante el período de estudio se documentaron múltiples instancias:

Celebraciones del cumpleaños de Hitler (20 de abril) con mensajes laudatorios, imágenes del dictador nazi, y referencias a su legado. Estos contenidos no presentan a Hitler como figura histórica objeto de estudio, sino como modelo, mártir o héroe.

Conmemoraciones de la quema de libros nazi (10 de mayo de 1933) presentada no como atrocidad a recordar críticamente, sino como acto justificado de “purificación cultural” frente a “degeneración”.

Santificación de autores de atentados terroristas, particularmente Elliot Rodger (autor de la masacre de Isla Vista, 2014, convertido en “santo” incel) y Anders Breivik (autor de la masacre de Noruega, 2011, celebrado en círculos extremistas). Estos individuos son presentados como mártires, héroes o modelos, con contenido que oscila entre la admiración explícita y la “comprensión” de sus actos.

Conmemoración instrumental de los atentados del 11 de septiembre (11-S), donde redes de propaganda afines a Al Qaeda relanzan fragmentos de sus reportajes audiovisuales fundacionales, ediciones especiales de revistas digitales y montajes de vídeo acompañados de nasheeds (cánticos religiosos) de corte bélico. Estos contenidos ensalzan la figura de los diecinueve operativos suicidas bajo la categoría de mártires legítimos y héroes, justificando la destrucción masiva como un acto necesario de castigo contra Occidente.

Glorificación de unidades militares fascistas responsables de crímenes de guerra, como la X Flottiglia MAS italiana. Estos contenidos no reconocen la naturaleza criminal de estas unidades, sino que las presentan como ejemplos de valentía, disciplina o patriotismo.

La gravedad de este patrón radica en su función normalizadora: acostumbra a la audiencia a la violencia extrema presentada bajo luz positiva, reduce inhibiciones morales, y en casos extremos puede inspirar imitación. Estudios sobre terrorismo han documentado sistemáticamente cómo perpetradores de atentados consumieron previamente contenido glorificador de violencia anterior.

Nivel de alarma: CRÍTICO. Cualquier contenido que glorifique violencia histórica debe ser considerado alta prioridad para moderación y, según contexto, notificación a autoridades.

Prevalencia por ideología: yihadismo y extrema derecha

Patrón 2: Amenazas específicas a personas identificadas

La transición desde discurso general de odio hacia amenazas dirigidas a individuos específicos representa una escalada significativa en la escala de riesgo. Durante el estudio se documentaron casos donde figuras públicas específicas (deportistas, políticos, activistas) eran nombradas con intención amenazante:

Mensajes del tipo “X será expulsado”, “van a retirar la custodia a Y”, formulados no como opinión o deseo, sino con tono de predicción o advertencia implícita. Aunque técnicamente no constituyen amenazas directas, el contexto y tono sugieren intimidación.

Referencias a direcciones, lugares de residencia, o rutinas de individuos específicos, información que solo tiene utilidad para localizar físicamente a la persona.

Uso de imágenes de personas específicas en fotomontajes degradantes, violentos o amenazantes, especialmente cuando se acompañan de texto sugestivo.

Este patrón requiere especial atención porque:

- Indica que el odio abstracto se ha concretado en objetivos específicos
- Crea entorno de intimidación que puede silenciar voces críticas
- Ha precedido históricamente a actos de violencia física
- Puede constituir delito (amenazas, acoso) dependiendo de formulación y legislación

Nivel de alarma: CRÍTICO. Estos contenidos deben ser documentados meticulosamente, preservando evidencia, y valorada su notificación tanto a las personas objetivo como a autoridades competentes.

Prevalencia por ideología: extrema derecha

Patrón 3: Lenguaje eliminacionista

El lenguaje eliminacionista se caracteriza por presentar la eliminación, expulsión o desaparición de grupos humanos completos como solución necesaria, deseable o inevitable. Este patrón se manifiesta mediante:

Lemas como “Remigración”, “Cannot coexist” (no podemos coexistir), “Invasión” (referido a migración), “Anular nacionalizaciones”. Estos términos comparten la caracterización de la presencia de determinados grupos (migrantes, minorías, etc.) como un problema que requiere una solución radical.

Uso de categorías dogmáticas excluyentes en el ámbito religioso, destacando términos como “kuffar” (infieles) o apóstatas (aquellos que han abandonado o traicionado la fe ortodoxa). Estas etiquetas despojan a los individuos de cualquier protección ética o legal dentro de la narrativa doctrinal, convirtiéndolos en objetivos legítimos de castigo o erradicación sistemática.

Referencias a “deportación masiva”, “expulsión”, “devolución” de poblaciones enteras, incluyendo frecuentemente descendientes nacidos en Europa, lo que implica proyectos de limpieza étnica.

Deshumanización mediante terminología que niega la humanidad plena: “invasores”, “reemplazadores”, o la equiparación con plagas y fenómenos naturales destructivos.

El lenguaje eliminacionista cumple una función preparatoria: normaliza progresivamente la idea de que determinados grupos humanos no deben o no pueden estar presentes, creando un clima ideológico que facilita la aceptación de medidas cada vez más radicales. Históricamente, los genocidios y las limpiezas étnicas han sido precedidos por períodos de normalización de lenguaje eliminacionista.

Nivel de alarma: CRÍTICO. Aunque el lenguaje eliminacionista per se puede estar protegido por libertad de expresión (dependiendo de formulación y jurisdicción), su presencia indica radicalización avanzada y debe ser tratado como indicador de riesgo máximo.

Prevalencia por ideología: yihadismo, extrema derecha

Patrón 4: Ideación suicida normalizada

Particularmente prevalente en comunidades incel, la normalización de ideación suicida constituye un patrón de gravedad extrema con implicaciones inmediatas para la salud pública. Se manifiesta mediante:

- Discusión de métodos suicidas con naturalidad, sin mostrar resistencia o búsqueda de alternativas.
- Presentación del suicidio como opción racional y comprensible, incluso recomendable (“assisted suicide” - suicidio asistido como opción para incels).
- Celebración o romantización de muertes por suicidio dentro de la comunidad.
- Lemas como “wasted life” (vida desperdiciada) que presentan la existencia como carente de valor o propósito.
- Ideología “blackpill” que, al postular que no hay posibilidad de mejora o cambio, conduce lógicamente a desesperanza absoluta.

Los datos de salud mental en estas comunidades son alarmantes: estudios recientes indican que aproximadamente el 75% de los hombres

que se identifican como incels sufren depresión moderada o grave (Costello et al., 2022). La comunidad online, lejos de ofrecer apoyo o perspectiva, refuerza y legitima la desesperanza mediante un proceso de contagio social.

Nivel de alarma: CRÍTICO. Este patrón requiere respuesta inmediata desde la salud mental. Profesionales que detecten este contenido deben considerar derivación a servicios de crisis, especialmente si observan progresión desde ideación vaga hacia planes concretos.

Prevalencia por ideología: incel y yihadismo

Patrón 5: Deslegitimación de democracia

La deslegitimación sistemática de instituciones, procesos y valores democráticos constituye un ataque a las estructuras que permiten la convivencia pacífica y la resolución no violenta de conflictos. Se manifiesta mediante:

- Rechazo de resultados electorales desfavorables, presentados como “fraudulentos” o “manipulados” sin evidencia.
- Ataques a medios de comunicación independientes mediante términos como “Lügenpresse” (prensa mentirosa), “fake news”, presentando como conspiración coordinada cualquier información que contradiga la narrativa extremista.
- Caracterización del “sistema” como intrínsecamente corrupto, irreformable, merecedor de destrucción más que de mejora.
- Legitimación de vías extra-democráticas: si el sistema es corrupto y las elecciones son fraudulentas, cualquier medio se vuelve justificable para “restaurar” la verdadera voluntad popular.

Este patrón es particularmente insidioso porque erosiona las bases del contrato social. Si significativas porciones de la población dejan de aceptar mecanismos democráticos como legítimos, las opciones restantes son autoritarismo o violencia.

Nivel de alarma: CRÍTICO. La deslegitimación de la democracia, especialmente cuando proviene de actores con representación institucional (partidos parlamentarios), representa amenaza existencial para sistemas políticos liberales.

Prevalencia por ideología: extrema derecha

Patrón 6: Antisemitismo sistemático

El antisemitismo contemporáneo frecuentemente se presenta mediante teorías conspirativas más que odio explícito, lo que puede dificultar su detección pero no reduce su gravedad. Se manifiesta mediante:

- Teorías de control oculto: bancos, medios de comunicación, gobiernos serían controlados por “élites judías” operando en sombras.
- Apropiación de teorías conspirativas históricas como los “Protocolos de los Sabios de Sion” (fraude antisemita de principios siglo XX) presentados como revelación de verdad histórica.
- “Teoría jázara”: negación de origen ancestral judío en Tierra Santa, presentando a judíos como conversores posteriores sin conexión histórica legítima, lo que sirve para deslegitimar Estado de Israel.
- Referencias a “intelectualismo judío pervertido”, “degeneración cultural judía”, “bolchevismo judío”, reproducciones casi literales de propaganda nazi.
- Uso de códigos: “(((nombre)))” (triple paréntesis) para marcar individuos o instituciones como judíos/controlados por judíos.

Se observa un repunte de la propaganda integrista motivado por factores geopolíticos recientes, documentándose que actualmente el antisemitismo dentro de la cosmovisión y la narrativa yihadista ha experimentado un incremento y una centralidad muy importantes desde el inicio del conflicto y la crisis humanitaria en Gaza (Observatorio de Estudios sobre Terrorismo, 2025). Esta coyuntura es instrumentalizada por las redes de captación para fundir el antisionismo político con el odio antisemita clásico, acelerando la movilización ideológica de jóvenes vulnerables a través de imágenes de sufrimiento masivo combinadas con consignas de venganza doctrinal.

La persistencia del antisemitismo como núcleo del pensamiento conspirativo extremista responde a su funcionalidad: permite explicar fenómenos complejos (globalización, cambio tecnológico, crisis económicas) mediante una narrativa simple de grupo malévolo operando coordinadamente.

El antisemitismo ha inspirado históricamente las formas más extremas de violencia, culminando en el Holocausto.

Nivel de alarma: CRÍTICO. El antisemitismo no es “solo otra forma de odio”: tiene una historia y una estructura que lo vinculan directamente con las formas más extremas de violencia genocida.

Prevalencia por ideología: yihadismo y extrema derecha

Patrón 7: Infraestructura de violencia

La construcción de capacidades físicas para ejercer violencia organizada constituye la transición desde el extremismo ideológico hacia la capacidad operativa. Se manifiesta mediante:

- Entrenamientos de combate o clubes de lucha (también llamados **“active clubs”** o **“fight clubs”**): clases de boxeo, artes marciales mixtas (MMA) y defensa personal organizadas específicamente para juventudes de grupos extremistas. Estos entrenamientos, aunque presentados como actividad deportiva, cumplen funciones de construcción de cohesión grupal, preparación física para enfrentamientos, normalización de la violencia física y generación de un sentimiento de pertenencia a una supuesta élite guerrera mediante:
- Adquisición o entrenamiento en el uso de armas, desde armas blancas hasta armas de fuego donde la legislación lo permite.
- Entrenamiento en tácticas de grupo: observadores (spotters) en manifestaciones para identificar a opositores, coordinación mediante comunicaciones cifradas y el uso de pirotecnia o bengalas como armas improvisadas.
- Creación de infraestructura física: centros sociales, gimnasios y clubes de combate que funcionan como espacios de socialización, reclutamiento y entrenamiento fuera de supervisión.
- Instrumentalización de disciplinas de combate: Las redes de captación yihadista utilizan perfiles deportivos especializados para preparar capacidades de asalto en entornos reales. Una muestra de ello es la detención en Madrid de dos expertos en artes marciales mixtas vinculados a redes de captación del Estado Islámico, quienes utilizaban

su cualificación profesional en gimnasios para atraer y adoctrinar a menores vulnerables.

- Radicalización del entorno aficionado deportivo: Se detecta un aumento sistemático de la violencia entre los hinchas radicales y los fanáticos de los clubes deportivos. Estas dinámicas se vinculan cada vez más con amenazas físicas en el interior de los estadios o en sus cercanías, operando en ocasiones de forma coordinada con redes locales de delincuencia común y crimen organizado.

Este patrón distingue a los grupos con ideología extremista que se limitan a una retórica en línea, de aquellos colectivos con capacidad operativa real para ejercer violencia organizada. Históricamente, las facciones armadas más lesivas han dependido de una infraestructura previa de entrenamiento para construir su capacidad destructiva en el entorno físico.

Nivel de alarma: ALTO. Aunque el entrenamiento físico no es ilegal per se, cuando se organiza específicamente por y para grupos extremistas, constituye señal de alerta que justifica monitorización intensificada.

Prevalencia por ideología: yihadismo y extrema derecha

Patrón 8: Salud mental deteriorada colectiva

Particularmente documentado en comunidades incel, el deterioro colectivo de salud mental representa tanto consecuencia como factor agravante del extremismo. Se manifiesta mediante:

- Síntomas compatibles con PTSD (estrés postraumático): hipervigilancia, evitación, rumiación obsesiva, flashbacks (en este caso, de rechazos románticos/sociales repetidamente revividos).
- Fenómeno de "spirals": ciclos de pensamiento obsesivo-compulsivo sobre la propia situación, incapacidad de desengancharse mentalmente del contenido de la comunidad.
- Aislamiento social extremo: reducción de contactos sociales reales hasta limitarse a interacciones online dentro de la comunidad, lo que crea dependencia y reduce exposición a perspectivas alternativas.
- "Wretchedness": término usado dentro de comunidades para describir estado de miseria psicológica extrema, vivida como permanente e irreversible.

- Depresión colectiva normalizada: los datos indican que aproximadamente el 75% de los incels autoidentificados cumplen criterios de depresión moderada o grave, un porcentaje extraordinariamente elevado que indica que la comunidad agrega a personas con una vulnerabilidad psicológica preexistente (Costello et al., 2022).

La comunidad, lejos de ofrecer apoyo hacia recuperación, funciona como cámara de eco que valida y refuerza patrones cognitivos disfuncionales. El “blackpill” (determinismo biológico absoluto) constituye esencialmente una narrativa depresiva colectiva que elimina la esperanza.

En el contexto yihadista, la intersección con el deterioro de la salud mental se manifiesta principalmente a través del perfil del actor solitario inspirado. La distinción técnica entre las diferentes modalidades de actuación en solitario es crucial para la prevención, corrigiendo el uso mediático erróneo del término “lobo solitario”:

El actor solitario inspirado (yihadismo contemporáneo). Este perfil define a los perpetradores de la mayoría de los ataques cometidos en suelo europeo en los últimos años. El individuo ejecuta la acción táctica por cuenta propia, pero no opera de manera autónoma. Su conducta está directamente inspirada, legitimada y, en ocasiones puede estar tutorizada a distancia por la propaganda de una matriz terrorista (como el Estado Islámico o Al Qaeda) que le proporciona manuales operativos y directrices estratégicas de cómo y dónde atentar. Es precisamente en este perfil de actores solitarios inspirados donde la literatura y los informes policiales documentan de forma recurrente una alta prevalencia de trastornos mentales y vulnerabilidades psiquiátricas previas.

El lobo solitario genuino (predominante en extrema derecha). A diferencia del anterior, el lobo solitario estricto desarrolla un proceso de radicalización ideológica y ejecuta su acción violenta sin mantener ningún tipo de contacto, vinculación, ni siquiera una relación de inspiración directa con las directrices de un grupo terrorista formal. Este fenómeno es estadísticamente residual en el terrorismo de matriz integrista y se atribuye de manera casi exclusiva a dinámicas de la extrema derecha y el supremacismo racial.

Cuando el yihadismo instrumentaliza a un actor solitario con problemas de salud mental, el proceso de captación sigue un patrón psicosocial específico:

- **Aislamiento y consumo compulsivo:** Un aislamiento social profundo antecede a la radicalización, el cual es llenado mediante el consumo masivo de propaganda digital en canales encriptados.
- **Conversión del fracaso en misión:** El integrismo ofrece una salida a la crisis de identidad del sujeto, transformando sus fracasos personales o patologías en una misión trascendente y heroica.
- **Validación digital y resignificación del suicidio:** La comunidad virtual normaliza la violencia y ofrece una validación constante al usuario. Esto permite canalizar la ideación suicida preexistente del individuo a través de la narrativa del martirio (shahada). De este modo, el algoritmo transmuta el suicidio convencional —estrictamente prohibido como pecado en el islam— en una muerte heroica recompensada con el paraíso.

Esta confluencia entre una salud mental deteriorada y la radicalización guiada representa un riesgo dual de homicidio y suicidio simultáneos, lo que exige abordar el fenómeno entendiendo que opera de forma conjunta como una patología psiquiátrica individual y como una amenaza de seguridad ideológica.

Nivel de alarma: ALTO. Este patrón requiere respuesta desde la salud mental pública. La radicalización online y crisis de salud mental están profundamente entrelazadas y requieren abordaje integrado.

Prevalencia por ideología: todas las ideologías extremistas

Patrón 9: Mesianismo político

La presentación del propio grupo como únicos salvadores posibles frente a una crisis existencial inminente constituye narrativa movilizadora que genera sentido de urgencia y justificación para medidas extremas. Se manifiesta mediante lemas como:

- “Nur AfD kann Deutschland retten” (Solo AfD puede salvar Alemania) - repetido sistemáticamente por este partido.
- “Solo nosotros salvamos”, “juventud europea tiene misión histórica”, “última generación que puede actuar”.

- Narrativas apocalípticas: “si no actuamos ahora, Europa desaparecerá”, “nuestros hijos vivirán en califato”, “sustitución irreversible en 20 años”.
- Caracterización de oponentes no como equivocados sino como traidores, colaboradores del mal, cómplices de genocidio.

El mesianismo político cumple función psicológica: eleva la pertenencia al grupo desde opción política a misión trascendente, lo que intensifica compromiso, justifica sacrificios, y genera disposición a medios extraordinarios. La lógica es: si realmente somos los únicos que podemos evitar catástrofe civilizacional, cualquier medio se vuelve justificable.

Nivel de alarma: ALTO. El mesianismo político intensifica el compromiso y puede facilitar escalada desde activismo a violencia si el grupo concluye que medios convencionales son insuficientes.

Prevalencia por ideología: extrema derecha

Patrón 10: Normalización de crímenes de guerra

La glorificación de unidades militares o eventos históricamente asociados con crímenes de guerra constituye una forma específica de normalización de la violencia extrema. Se documenta mediante:

- Referencias laudatorias a X Flottiglia MAS (unidad naval fascista italiana responsable de crímenes de guerra documentados), presentada como modelo de valentía o patriotismo sin reconocimiento de su naturaleza criminal.
- Celebración de la Marcha sobre Roma (golpe de Estado fascista de 1922) como evento heroico, no como subversión violenta de la democracia.
- Reivindicación de unidades Waffen-SS, colaboracionistas con nazis en países ocupados, presentadas como defensoras de Europa frente al bolchevismo.

Este patrón es particularmente preocupante en contexto europeo, donde el consenso de posguerra sobre inaceptabilidad del fascismo y nazismo es fundacional para la construcción europea. Su cuestionamiento

no es meramente histórico, sino que desafía bases normativas del orden democrático liberal.

Nivel de alarma: ALTO. La normalización de los crímenes históricos prepara el terreno psicológico para la aceptación de atrocidades contemporáneas.

Prevalencia por ideología: yihadismo y extrema derecha

Patrón 11: Convergencia de múltiples odios

La acumulación de múltiples targets de odio en un mismo discurso o actor (racismo + antisemitismo + misoginia + homofobia + islamofobia) constituye un indicador de la radicalización particularmente profunda. Se manifiesta mediante:

- “Paquetes” ideológicos de ultra-derecha donde oposición a migración se combina automáticamente con anti-LGTBIQ+, antifeminismo, antisemitismo, etc.
- Construcción de enemigo total: no solo migrantes o musulmanes, sino también izquierda, feministas, LGTBIQ+, judíos, élites, medios, etc. generando cosmovisión paranoica donde el propio grupo está asediado por múltiples enemigos coordinados.
- Teorías conspirativas omniabarcantes que conectan todos los “enemigos” en un plan único de destrucción.

La convergencia de múltiples odios indica:

- Adopción de cosmovisión ideológica completa (no solo prejuicio aislado).
- Mayor probabilidad de violencia (más targets = más potenciales víctimas).
- Menor probabilidad de persuasión (no es opinión aislada sino sistema de creencias entero).
- Mayor aislamiento social (conflicto con múltiples grupos simultáneamente).

Nivel de alarma: CRÍTICO. La convergencia múltiple distingue prejuicio común de radicalización ideológica profunda.

Prevalencia por ideología: todas las ideologías extremistas

Patrón 12: Victimización de perpetradores

La inversión moral mediante la cual los perpetradores de violencia son presentados como víctimas constituye una estrategia retórica que desactiva la resistencia moral y legítima la violencia. Se manifiesta mediante:

- Presentación de agresores sexuales como víctimas de “cancel culture” o “feminismo extremista” (caso Rubiales en España usado como ejemplo de “persecución” del hombre).
- Caracterización de Hitler como “víctima” de agresión internacional, Tratado de Versalles, conspiración judía, eliminando su agencia como perpetrador de genocidio.
- Fascismo presentado como “perseguido” por narrativa histórica “injusta”, negando o minimizando sus crímenes mientras se enfatiza su “represión” posterior.
- Terroristas de extrema derecha presentados como desesperados que “no tenían otra opción” frente a “invasión” o “genocidio blanco”, retórica que desplaza responsabilidad moral desde perpetrador hacia víctimas o sociedad.

Esta inversión cumple función de desactivación de empatía hacia víctimas reales mientras se genera empatía hacia perpetradores. Si el violento es realmente la víctima, su violencia se vuelve comprensible, justificable, incluso admirable.

Nivel de alarma: MEDIO-ALTO. Este patrón es particularmente insidioso porque opera sobre mecanismos emocionales (empatía) más que racionales, haciéndolo efectivo incluso con audiencias educadas.

Prevalencia por ideología: todas la ideologías extremistas



12 PATRONES PELIGROSOS

SEÑALES DE ALARMA EN EXTREMISMO ONLINE

#	PATRON	NIVEL	DESCRIPCIÓN
1 	GLORIFICACIÓN VIOLENCIA	CRÍTICO	Celebración Hitler, atentados (Rodger, Breivik) como mártires. Normaliza violencia extrema, reduce inhibiciones.
2 	AMENAZAS ESPECÍFICAS	CRÍTICO	Personas nombradas con intención amenazante. Referencias a direcciones/rutinas. Odio concretado en objetivos.
3 	LENGUAJE ELIMINACIONISTA	CRÍTICO	"Remigración", "invasión", "no podemos coexistir". Presenta eliminación de grupos como solución necesaria.
4 	IDEACIÓN SUICIDA	CRÍTICO	Métodos naturalizados, suicidio como opción racional. 75% incels con depresión. Comunidad refuerza desesperanza.
5 	DESLEGITIMACIÓN DEMOCRACIA	CRÍTICO	Elecciones "fraudulentas", "Lügenpresse", sistema corrupto. Legitimación de vías extra-democráticas.
6 	ANTISEMITISMO SISTEMÁTICO	CRÍTICO	Control oculto, Protocolos Sion, [[[nombre]]]. Núcleo conspirativo vinculado a violencia genocida histórica.
7 	INFRAESTRUCTURA VIOLENCIA	ALTO	Entrenamientos combate, armas, tácticas grupo, centros sociales. Transición ideología a capacidad operativa.
8 	DETERIORO MENTAL COLECTIVO	ALTO	PTSD, "spirals", aislamiento extremo, depresión colectiva. Comunidad como cámara de eco disfuncional.
9 	MESIANISMO POLÍTICO	ALTO	"Solo nosotros salvamos", narrativas apocalípticas, última oportunidad. Genera urgencia y justifica medios extremos.
10 	NORMALIZACIÓN CRÍMENES GUERRA	ALTO	Glorificación X Flotiglia MAS, Waffen-SS, Marcha sobre Roma. Desafía bases normativas democráticas.
11 	CONVERGENCIA MÚLTIPLES ODIOS	MEDIO- ALTO	Racismo + antisemitismo + misoginia + homofobia simultáneos. Indica radicalización profunda, no prejuicio aislado.
12 	VICTIMIZACIÓN PERPETRADORES	MEDIO- ALTO	Agresores como "víctimas" (Rubiales, Hitler). Inversión moral que desactiva empatía hacia víctimas reales.

CRITERIOS DE EVALUACION DE RIESGO

PROXIMIDAD A VIOLENCIA | FRECUENCIA DE APARICION | RESISTENCIA A INTERVENCION | ESCALABILIDAD MASIVA | IRREVERSIBILIDAD DEL DAÑO



PERFILES VULNERABLES A LA RADICALIZACIÓN

1. Introducción: complejidad de la categorización en la Era Digital

El análisis sistemático de las diecisiete variables de categorización aplicadas a la muestra de contenido extremista permite identificar los perfiles demográficos, psicosociales y comportamentales que constituyen las audiencias prioritarias del discurso radicalizador. Comprender estos perfiles resulta esencial para el diseño de estrategias de prevención diferenciadas que atiendan a las vulnerabilidades específicas de cada población objetivo.

Sin embargo, es fundamental reconocer desde el inicio que los objetivos vulnerables a la radicalización extremista no son fáciles de categorizar mediante taxonomías rígidas o perfiles estáticos. La investigación documentó un predominio significativo del perfil del “lobo solitario”: individuos que se radicalizan mediante el consumo digital aislado, sin pertenencia formal a una organización estructurada, sin contacto personal con reclutadores activos y, frecuentemente, sin que su entorno inmediato detecte el proceso hasta etapas muy avanzadas. Adicionalmente, se identificaron múltiples casos que desafían completamente cualquier intento de categorización dentro de los marcos analíticos convencionales, evidenciando que la vulnerabilidad opera mediante combinaciones prácticamente infinitas de factores individuales y contextuales.

Más aún, la realidad contemporánea es que, a día de hoy, cualquier persona con acceso a internet es potencialmente vulnerable a la radicalización online. **Ya no existen fronteras geográficas que limiten la exposición al contenido extremista**, no existen barreras idiomáticas infranqueables gracias a la traducción automatizada y al contenido visual que trasciende el lenguaje, y no existen filtros socioeconómicos robustos, dado que los smartphones y la conexión a internet han alcanzado una penetración prácticamente universal. La radicalización online es un fenómeno genuinamente global que opera sin respetar las fronteras nacionales, las divisiones de clase o las categorías demográficas tradicionales.

Dicho esto, el análisis empírico de la muestra permite identificar dos perfiles principales que, sin ser exhaustivos ni mutuamente excluyentes, capturan las tendencias mayoritarias observadas en el contenido extremista analizado. Estos perfiles representan las poblaciones hacia las cuales el contenido extremista se dirige estratégicamente y donde las características específicas del desarrollo, del contexto social y del entorno digital convergen para aumentar la vulnerabilidad.

2. Características comunes a perfiles vulnerables

Antes de detallar perfiles específicos, el análisis revela características transversales que aparecen consistentemente en audiencias objetivo del extremismo digital, independientemente de la edad exacta o el contexto particular.

Demografía: masculinidad y juventud como factores centrales

El análisis de la variable “Audiencia” en la muestra revela que el contenido extremista está dirigido fundamentalmente a los “hombres”, los “jóvenes adultos” (de dieciocho a treinta años) y los “adolescentes” (de doce a diecisiete años). Esta concentración demográfica no es accidental, sino el reflejo de un targeting estratégico por parte de los actores extremistas que identifican en esta demografía características específicas que facilitan la captación y la radicalización. Los tres perfiles identificados son igualmente preocupantes para los equipos de intervención, ya que cada grupo presenta vulnerabilidades particulares que los radicalizadores explotan de forma diferenciada: mientras que los menores y los adolescentes muestran una menor madurez cognitiva y una mayor permeabilidad ante los formatos gamificados, los jóvenes adultos disponen de una mayor capacidad de movilidad y autonomía operativa para transitar desde la militancia digital hacia la acción violenta material.

La masculinidad constituye un factor transversal absolutamente dominante. El contenido de extrema derecha se dirige predominantemente a los hombres, especialmente a los jóvenes adultos y adolescentes, presentando narrativas de una masculinidad amenazada que requiere una “defensa” activa mediante el activismo político o la violencia. El contenido misógino asociado al movimiento incel se dirige exclusivamente a los hombres por definición ideológica, construyendo una identidad colectiva basada en una victimización compartida por las mujeres y por un sistema que supuestamente las privilegia. Incluso el contenido que no es explícitamente “masculinista” en su temática emplea una estética visual, unas referencias culturales y unos marcos narrativos que asumen a la audiencia masculina como destinataria primaria.

En el contexto del extremismo yihadista, existe un predominio del targeting hacia los hombres jóvenes mediante narrativas de masculinidad

guerrera, hermandad entre combatientes y honor recuperado mediante la lucha. La masculinidad se convierte en un vector de vulnerabilidad que trasciende las ideologías específicas, operando como una constante en el extremismo de derecha, la misoginia incel y el yihadismo.

La edad resulta igualmente crítica como factor de vulnerabilidad. Los jóvenes adultos (de dieciocho a treinta años) y los adolescentes (de doce a diecisiete años) comparten características psicosociales que aumentan la susceptibilidad a la radicalización: se encuentran en un período crucial de formación de identidad donde los individuos buscan activamente marcos ideológicos y comunitarios que den un sentido coherente a su experiencia vital; manifiestan una mayor apertura a las ideas nuevas o transgresivas como forma de diferenciación respecto a la generación anterior y de construcción de una identidad distintiva; poseen una menor experiencia vital acumulada que proporcionaría un contexto histórico, una capacidad para detectar la manipulación o un escepticismo desarrollado mediante decepciones previas; y, crucialmente, pasan significativamente más tiempo en las plataformas digitales donde la exposición algorítmica al contenido extremista es más probable y más sostenida.

Hiperconectividad digital: cantidad y calidad

El perfil vulnerable contemporáneo se caracteriza fundamentalmente por la hiperconectividad digital: múltiples horas diarias (frecuentemente cinco o más) en redes sociales, plataformas de video, foros, aplicaciones de mensajería, o espacios de gaming. Esta hiperconectividad no es meramente cuantitativa (tiempo total en pantalla) sino cualitativamente diferente: las interacciones digitales ocupan la centralidad en la vida social, afectiva, e identitaria que históricamente correspondía a interacciones presenciales.

Crucialmente, esta generación hiperconectada es la primera que normaliza la violencia mediante consumo digital constante. Esta normalización se manifiesta mediante múltiples vectores: memes que presentan violencia como humor aceptable; videos virales de peleas callejeras, confrontaciones políticas, o agresiones que circulan sin contexto ni condena; estética de “fight clubs” y “active clubs” (grupos de extrema derecha que entrenan combate) presentada como aspiracional; cultura de hinchas de fútbol violentos glorificada mediante videos y fotografías; y gaming donde la violencia es mecánica central de entretenimiento. Esta exposición repetida reduce

el umbral de shock ante violencia real, facilitando la transición desde el consumo de violencia digital hacia la participación en violencia física cuando la narrativa extremista la presenta como justificada.

Durante el período de formación de identidad (adolescencia, juventud temprana), individuos históricamente construían sentido de sí mismos mediante interacciones presenciales con pares, familia extendida, instituciones educativas, organizaciones comunitarias, y espacios de socialización física. **La hiperconectividad digital desplaza parcialmente estas interacciones formativas hacia espacios online donde las dinámicas son fundamentalmente diferentes:**

- Las señales sociales son significativamente más ambiguas debido a ausencia de lenguaje corporal, tono vocal, expresión facial, y contexto situacional que proporcionan información crucial para la interpretación de comunicación. Esta ambigüedad facilita malentendidos, pero también permite que contenido extremista sea consumido sin resistencia social inmediata que la comunicación presencial proporcionaría.
- El contenido está algorítmicamente cuidado para maximizar engagement (tiempo de visualización, interacciones, retorno a plataforma) sin consideración alguna de si contenido promueve desarrollo psicológico saludable, pensamiento crítico, o bienestar del usuario. Algoritmos optimizan para métricas de negocio, no para salud mental o resistencia a extremismo.
- La exposición a voces extremas es estructuralmente más probable que en interacción presencial. En contextos físicos, personas con opiniones genuinamente extremas constituyen minoría estadística que la mayoría moderada tiende a marginalizar o ignorar. Online, estas voces minoritarias pueden ser amplificadas artificialmente mediante bots, cuentas coordinadas, y crucialmente algoritmos que detectan que contenido controvertido genera engagement alto y consecuentemente lo promueven a audiencias masivas.
- Las consecuencias sociales de transgresión son significativamente menores debido a anonimato (o pseudo-anonimato mediante nombres de usuario), posibilidad de crear múltiples identidades digitales y abandonar aquellas que generan reputación negativa, y ausencia de

repercusiones en vida offline que moderarían comportamiento extremo en contextos presenciales.

Literacidad digital: asimetría crítica

Los jóvenes hiperconectados desarrollan una literacidad digital técnica considerable: saben navegar las plataformas con fluidez, emplear múltiples aplicaciones simultáneamente, crear y compartir contenido mediante herramientas de edición y dominar las convenciones comunicativas de cada espacio digital específico. Sin embargo, frecuentemente carecen de una literacidad digital crítica: la capacidad de evaluar la credibilidad de las fuentes, detectar la manipulación mediante técnicas retóricas o visuales, comprender las lógicas algorítmicas que determinan qué contenido ven, identificar bots frente a humanos, reconocer campañas coordinadas de desinformación o analizar los incentivos económicos y políticos detrás del contenido que consumen.

Esta asimetría entre la competencia técnica y la competencia crítica los hace particularmente vulnerables al contenido extremista que emplea una sofisticación técnica (memes profesionalmente producidos con una edición de calidad, vídeos con una cinematografía impresionante y música emocional, textos con apariencia de rigor académico mediante la citación selectiva e infografías visualmente impactantes con datos descontextualizados) para transmitir mensajes extremistas. La producción profesional confiere una credibilidad perceptual: el contenido que “se ve profesional” es interpretado inconscientemente como más creíble que el contenido amateur, independientemente de su veracidad real.

3. Perfil de vulnerabilidad primario: varón joven adulto (18-30 años) digitalmente hiperconectado

El primer perfil de alta vulnerabilidad concentra hombres en rango de edad dieciocho a treinta años, período que corresponde a la transición desde la adolescencia hacia la adultez establecida, caracterizada por toma de decisiones formativas sobre la trayectoria educativa, profesional, y personal, y la búsqueda de identidad adulta diferenciada de la familia de origen.

Factores psicosociales agravantes de vulnerabilidad

Dentro de la demografía joven-masculina-hiperconectada, ciertos factores psicosociales aumentan la vulnerabilidad dramáticamente cuando aparecen individual o combinadamente:

Aislamiento social. Los individuos con unas redes sociales presenciales limitadas (pocos o ningún amigo cercano, relaciones familiares tensas o cortadas, y dificultades de integración en el entorno escolar o laboral debido a la personalidad, a las diferencias culturales o al rechazo activo) buscan desesperadamente una pertenencia en las comunidades online. Las comunidades extremistas ofrecen una aceptación inmediata e incondicional basada exclusivamente en una identidad compartida (racial, nacional, de género o religiosa) sin requerir una vulnerabilidad emocional, una construcción gradual de confianza mediante la reciprocidad o una inversión de tiempo que caracteriza a las amistades presenciales saludables. Esta facilidad de acceso a una pertenencia comunitaria hace que el extremismo online sea psicológicamente atractivo para las personas socialmente aisladas.

Frustración económica o de estatus. Los jóvenes adultos que experimentan una movilidad social descendente (una situación económica objetivamente peor que la que sus padres tenían a una edad equivalente), un estancamiento prolongado (la educación superior, incluyendo los títulos universitarios, no se traduce en un empleo acorde con las expectativas ni en unos ingresos suficientes para la independencia) o una precariedad laboral crónica (los contratos temporales, el subempleo o el trabajo en sectores con un declive estructural) son extremadamente receptivos a las narrativas que externalizan la responsabilidad de esta situación. La extrema derecha ofrece una explicación simplificada, pero psicológicamente satisfactoria: “tu situación no es tu culpa ni refleja tus capacidades; es causada por los migrantes que roban empleos, las élites globalistas que traicionan a los trabajadores nacionales o el feminismo que privilegia a las mujeres en el mercado laboral”. Esta narrativa resulta psicológicamente atractiva porque preserva la autoestima y el sentido de competencia personal, mientras proporciona un objetivo externo identificable sobre el cual proyectar la frustración.

Fracaso romántico y sexual. Particularmente relevante para la vulnerabilidad específica a la ideología incel, aunque también opera en la

extrema derecha. Los jóvenes con dificultades sostenidas para establecer relaciones románticas o experiencias sexuales, especialmente si atribuyen estas dificultades a factores percibidos como completamente fuera de su control personal (una apariencia física considerada no atractiva, una altura por debajo de la media cultural, características faciales específicas o una timidez patológica), son extremadamente receptivos a las narrativas de determinismo biológico que presentan su situación como inevitable e inmutable. La ideología “Blackpill” proporciona un marco cognitivo que simultáneamente valida su experiencia subjetiva de rechazo (“no estás loco, el problema es real y observable”) y elimina completamente la agencia personal (“no hay absolutamente nada que puedas hacer para cambiar tu situación; la mejora es imposible”), conduciendo a una desesperanza nihilista, una depresión severa y una ideación suicida normalizada dentro de la comunidad.

Exposición previa a violencia o trauma. Los jóvenes con historias personales de victimización (bullying sostenido durante los años escolares, abuso físico o emocional en la familia, exposición a la violencia doméstica o comunitaria, o trauma derivado de un conflicto bélico en el caso de los refugiados) pueden sentirse atraídos por las narrativas extremistas que validan su ira acumulada y presentan la violencia como una respuesta legítima, necesaria o incluso moralmente obligatoria. Las comunidades extremistas ofrecen marcos ideológicos donde el trauma personal individual se reinterpreta como una manifestación de una victimización grupal sistemática (racial, nacional, religiosa o de género) que justifica una venganza colectiva. El extremismo transforma el dolor personal en una causa política, proporcionando sentido y propósito a un sufrimiento que, de otro modo, parecería aleatorio y sin significado.

Indicadores comportamentales de radicalización progresiva

En individuos que corresponden al perfil vulnerable, la radicalización temprana se manifiesta mediante cambios observables que familiares, educadores, o empleadores pueden potencialmente detectar si están atentos:

Cambio dramático en consumo de medios. Se observa una transición desde el consumo de contenido diverso procedente de múltiples fuentes con perspectivas variadas hacia un consumo predominante

o exclusivo de contenido procedente de fuentes específicas (canales particulares de YouTube, cuentas específicas de Instagram o canales de Telegram) con una orientación ideológica consistente y progresivamente más radical. Simultáneamente, aparece un rechazo explícito y hostil de las fuentes mainstream, caracterizadas despectivamente como “mentirosas”, “manipuladas por las élites” o “propaganda del sistema”, sin capacidad para distinguir entre una crítica legítima a los sesgos mediáticos y un rechazo total de toda información que contradiga la narrativa extremista.

Adopción de lenguaje codificado extremista. El uso casual en la conversación de términos, referencias o memes que no son comprensibles fuera de una subcultura extremista específica constituye otro indicador relevante. En la extrema derecha: “remigración”, “Gran Reemplazo”, “identitarios”, “despiertos versus dormidos”, “bluepill/redpill” o referencias numéricas como “1488”. En la comunidad incel: “Blackpill”, “Chad”, “Stacy”, “truecel”, “lookism” o “hypergamy”. Este lenguaje marca la pertenencia a una comunidad iniciada y señala a otros miembros el nivel de radicalización alcanzado.

Cambio en presentación personal y estética. La adopción de una vestimenta, una simbología, unos cortes de cabello o una gestualidad asociados con una subcultura extremista específica constituye otra señal relevante. En el contexto de la extrema derecha juvenil europea, esto incluye frecuentemente una estética “fitness/sigma”: un énfasis obsesivo en el desarrollo muscular visible, una vestimenta deportiva de marcas específicas asociadas con el movimiento (ciertas marcas de ropa de combate o streetwear con códigos específicos), y una postura corporal y una gestualidad que proyectan dominancia física. En algunos casos, aparecen tatuajes con una simbología extremista (runas nórdicas apropiadas por los nazis, números codificados o símbolos históricos fascistas, entre otros).

Aislamiento progresivo de redes sociales previas. Se observa una reducción del contacto con los amigos de la infancia o de la adolescencia, un distanciamiento de los familiares que no comparten la cosmovisión radicalizante, el abandono de actividades sociales previamente disfrutadas y el rechazo de conocidos del trabajo o de los estudios. Este aislamiento puede ser voluntario (el individuo que se radicaliza encuentra las interacciones con

los “normies”¹⁵ frustrantes, aburridas o moralmente comprometedoras) o el resultado de un rechazo activo por parte de la red social previa, que observa cambios ideológicos y comportamentales preocupantes y decide cortar el contacto.

Expresión de ideas extremistas con creciente apertura. Inicialmente, el individuo en proceso de radicalización puede expresar las ideas extremistas de manera tentativa, mediante el “humor” que permite una negación plausible (“era solo una broma”) o en contextos donde anticipa acuerdo. Con la progresión temporal, la expresión se vuelve más abierta, directa, confrontacional y completamente resistente a la contestación o al debate. Puede evolucionar hacia confrontaciones activas donde el individuo busca deliberadamente “redpillear” (radicalizar) a otros, interpretando la resistencia como una evidencia de que los demás están “dormidos” o “manipulados”, en lugar de considerar que sus posiciones podrían ser incorrectas.

Participación en actividad grupal offline. La asistencia documentable a manifestaciones extremistas, eventos de formación ideológica, entrenamientos físicos organizados por grupos extremistas (las sesiones de boxeo de Blocco Studentesco o la defensa personal promovida por Falange Española de las JONS) o reuniones presenciales en centros sociales extremistas constituye otro indicador relevante. Esta transición desde un activismo puramente online hacia la participación presencial en actividades grupales indica una consolidación profunda del compromiso ideológico y representa una escalada significativa en el nivel de riesgo, ya que la participación física requiere una inversión de tiempo, recursos y energía sustancialmente mayor que el consumo digital pasivo, generando un compromiso psicológico mediante la disonancia cognitiva (“he invertido tanto que el movimiento debe valer la pena”).

¹⁵ En la cultura e iconografía de las comunidades virtuales y foros de internet, el término “normie” se utiliza de manera peyorativa para describir a las personas comunes que no pertenecen a una subcultura específica, consumen cultura de masas y aceptan las normas sociales mayoritarias sin cuestionarlas (Sugiura, 2021). En los procesos de radicalización, esta etiqueta cumple una función de aislamiento psicosocial: al categorizar al entorno familiar o de amistades previas como normies, el individuo traza una frontera de superioridad moral y cognitiva, descalificando cualquier crítica o contraargumento externo por considerarlo fruto de la ignorancia o del adoctrinamiento del sistema.

4. Perfil de vulnerabilidad secundario: adolescente (12-17 años) en crisis de identidad hiperconectado

Los adolescentes en el rango de edad de doce a diecisiete años constituyen una población de particular vulnerabilidad debido a la convergencia de características específicas de la etapa de desarrollo psicológico con la hiperconectividad digital, en un contexto donde la supervisión adulta efectiva del consumo online es frecuentemente inadecuada o completamente ausente.

Este perfil resulta especialmente preocupante por dos razones críticas: primero, representa el segmento demográfico de más rápido crecimiento en los casos de radicalización documentados durante los últimos años (Capítulo 4. Observatorio Internacional de Estudios sobre Terrorismo, 2025), evidenciando una tendencia alarmante de rejuvenecimiento del extremismo violento que anteriormente afectaba predominantemente a los adultos jóvenes (de dieciocho a treinta años); segundo, su condición de menores de edad genera complejidades legales y procesales específicas, dado que los sistemas de justicia juvenil europeos están diseñados para la delincuencia común (los hurtos, el vandalismo o el consumo de sustancias) y carecen frecuentemente de marcos apropiados para abordar la radicalización ideológica y la planificación de violencia terrorista en menores, creando un vacío entre la gravedad de la amenaza y la capacidad institucional de una respuesta proporcional que respete simultáneamente los derechos del menor y la seguridad pública.

Características de vulnerabilidad específica adolescente

Búsqueda de identidad como tarea central de desarrollo. La adolescencia se caracteriza fundamentalmente por una exploración activa de las identidades posibles, las ideologías políticas y filosóficas, y las pertenencias grupales como un proceso completamente normativo del desarrollo psicológico. Los adolescentes se preguntan existencialmente “¿quién soy?” y experimentan con múltiples respuestas. Las comunidades extremistas ofrecen una identidad “lista para usar” con una máxima claridad moral absoluta (nosotros versus ellos, el bien versus el mal, y la verdad versus la mentira) sin ambigüedad ni complejidad. Esta simplicidad puede resultar extremadamente atractiva para los adolescentes abrumados por la complejidad de la construcción identitaria genuina en una sociedad pluralista donde múltiples caminos son posibles y ninguno viene con garantías.

Susceptibilidad amplificada a presión de pares digitalizada.

Los adolescentes son evolutivamente hipersensibles a la aprobación o al rechazo de sus pares como mecanismo de aprendizaje social. En el contexto digital, esta sensibilidad se amplifica dramáticamente porque el engagement (likes, comentarios, shares y seguidores) proporciona una cuantificación visible, pública y constantemente actualizada de la aceptación social. El contenido extremista que genera un engagement alto puede ser compartido o reproducido por adolescentes que buscan validación social dentro de su grupo de pares, iniciando un proceso de adopción ideológica que comienza como una performance para impresionar o pertenecer, pero que puede progresivamente internalizarse mediante la repetición y el refuerzo.

Pensamiento abstracto y crítico en desarrollo. La capacidad de pensamiento complejo, la consideración simultánea de múltiples perspectivas, la evaluación matizada de evidencia contradictoria y la detección de falacias lógicas se desarrollan progresivamente durante la adolescencia, no estando completamente consolidadas hasta la adultez temprana. Los adolescentes tempranos y medios (de doce a quince años) frecuentemente presentan dificultades significativas para detectar falacias lógicas sofisticadas, evaluar la credibilidad de las fuentes mediante triangulación o resistir argumentos emocionalmente persuasivos, pero lógicamente débiles, que caracterizan a la propaganda extremista profesional.

Transgresión como exploración normativa de límites. La adolescencia normalmente incluye cierto grado de transgresión (el desafío a la autoridad parental y escolar, la experimentación con los límites sociales y la puesta a prueba de las normas) como una parte completamente saludable del proceso de individuación y construcción de autonomía. El contenido extremista puede resultar atractivo precisamente porque es transgresivo, “prohibido” y explícitamente rechazado por los adultos y las autoridades, sin que el adolescente necesariamente adhiera genuinamente al contenido ideológico, sino disfrutando del propio acto de transgresión como una afirmación de independencia.

Vulnerabilidad de autoestima como factor agravante crítico. Los adolescentes con baja autoestima, depresión clínica, trastornos de la conducta alimentaria, ideación suicida o trauma no procesado constituyen una población de vulnerabilidad particularmente extrema. Los radicalizadores

buscan deliberadamente esta **dobles vulnerabilidad** (la adolescencia combinada con una crisis psicológica) porque estos jóvenes están desesperados por encontrar pertenencia, validación y marcos que den sentido a su sufrimiento. Las comunidades extremistas ofrecen una aceptación inmediata sin juicio, validan las experiencias de rechazo o trauma y proporcionan narrativas que externalizan completamente la responsabilidad del sufrimiento psicológico (“no es tu culpa, es culpa de una sociedad corrupta/del feminismo/de la inmigración/del sistema”). Para un adolescente en crisis, este paquete puede resultar psicológicamente irresistible.

Contextos de mayor riesgo para población adolescente

Entornos educativos con bajo sentido de pertenencia. Los adolescentes que experimentan un aislamiento social sostenido o una marginación activa en los contextos escolares (bullying sistemático, exclusión deliberada de los grupos sociales, conflicto crónico con la autoridad escolar o un rendimiento académico muy bajo que genera vergüenza) buscan desesperadamente comunidades alternativas donde experimentar pertenencia. Las comunidades extremistas online ofrecen una aceptación inmediata, sin requisitos ni juicio, además de marcos ideológicos que reinterpretan la exclusión escolar como una evidencia de superioridad intelectual o moral (“eres rechazado porque eres más inteligente/más despierto que los ‘normies’ conformistas”).

Exposición temprana no supervisada a contenido adulto. Los adolescentes con un acceso completamente no supervisado a internet desde edades muy tempranas (nueve o diez años) pueden ser expuestos a contenido extremista, violento o sexual antes de haber desarrollado la capacidad cognitiva y emocional necesaria para procesarlo críticamente. Los algoritmos de recomendación no distinguen a los usuarios por edad emocional o cognitiva, tratando a un adolescente de trece años de manera idéntica a un adulto de treinta, y exponiendo consecuentemente a los adolescentes a un contenido diseñado para audiencias adultas con un contexto y una resistencia crítica que ellos todavía no poseen.

Conflicto familiar sobre autonomía digital. Las familias donde existen tensiones significativas sobre el uso de la tecnología presentan riesgos en ambos extremos del espectro de control. En las familias con restricciones percibidas como excesivamente autoritarias (una monitorización que el

adolescente experimenta como invasiva o prohibiciones totales sin una explicación razonada), el adolescente puede buscar activamente espacios digitales completamente ocultos a la supervisión parental, aumentando la probabilidad de exposición a contenido extremista en plataformas menos mainstream donde la moderación es mínima. Simultáneamente, en los entornos familiares donde el control es completamente nulo (padres sin conocimiento técnico, sin tiempo o sin interés en supervisar el consumo digital de sus hijos), existe un riesgo elevado de que un niño ya vulnerable por otros factores busque apoyo en entornos digitales de radicalización donde encuentre un refuerzo inmediato, incondicional y una validación de pensamientos y emociones que la familia no proporciona.



CONSIDERACIÓN ESPECIAL: YIHADISMO Y POBLACIÓN ADOLESCENTE MUSULMANA

Aunque esta investigación no accedió de manera significativa a espacios de radicalización yihadista debido a su naturaleza técnicamente inaccesible mediante métodos OSINT convencionales, la literatura académica existente documenta que los adolescentes musulmanes en el contexto europeo enfrentan vulnerabilidades específicas adicionales. La experiencia de discriminación, islamofobia, marginación social y económica, crisis de identidad bicultural (la tensión entre la cultura familiar musulmana y la cultura mayoritaria europea) y la búsqueda de pertenencia comunitaria pueden ser explotadas por los reclutadores yihadistas mediante narrativas de victimización colectiva musulmana, pureza religiosa frente a corrupción occidental y hermandad global de creyentes. El perfil vulnerable combina la edad adolescente, la identidad musulmana, la experiencia de discriminación o marginación, la crisis de pertenencia y la exposición al contenido yihadista mediante las redes sociales o los contactos personales que operan como puentes hacia espacios clandestinos de radicalización más profunda.

5. Diferencias fundamentales entre vulnerabilidad adolescente y adulta

El análisis de las trayectorias de radicalización documentadas durante esta investigación, complementado con entrevistas a especialistas de las fuerzas de seguridad, revela diferencias fundamentales entre cómo los menores (de doce a diecisiete años) y los adultos jóvenes (de dieciocho a treinta años) experimentan los procesos de radicalización online. Estas diferencias no son meramente cuantitativas (más o menos tiempo online), sino cualitativamente distintas en términos de motivaciones, velocidad de radicalización, profundidad ideológica y tipo de contenido consumido.

Comprender estas diferencias es crítico para el diseño de intervenciones preventivas efectivas, dado que las estrategias que funcionan con los adolescentes (los límites del tiempo de pantalla, la supervisión parental o la alfabetización mediática básica) pueden ser insuficientes o inapropiadas para los adultos jóvenes, quienes requieren un engagement ideológico más profundo y un abordaje de los factores materiales de frustración que hacen que las narrativas extremistas resulten psicológicamente atractivas.

Velocidad versus profundidad. Expertos en terrorismo de la Guardia Civil señalan que la radicalización de menores se produce mediante una formulación aparentemente contradictoria: “es un proceso de muchas horas en internet, pero muy rápido”. Esta paradoja captura una dualidad fundamental: los menores pasan un volumen extremadamente alto de tiempo online (seis a diez horas diarias durante los fines de semana y las vacaciones no es infrecuente), exponiéndose a contenido radicalizador de manera intensiva durante un período breve (semanas o pocos meses), pero con una profundidad de comprensión ideológica frecuentemente superficial.

Un adolescente puede transitar desde el primer contacto con contenido político (un vídeo viral sobre inmigración o un meme sobre feminismo) hasta un consumo diario de propaganda extremista explícita en cuestión de cuatro a ocho semanas mediante una exposición algorítmica intensiva. Los algoritmos de recomendación detectan el engagement (el tiempo de visualización, los clicks o las búsquedas relacionadas) y aceleran la radicalización mostrando un contenido progresivamente más extremo, sin pausas. Sin embargo, cuando se entrevista a un menor radicalizado sobre los fundamentos ideológicos de las creencias que expresa, sus respuestas frecuentemente **revelan una comprensión limitada a slogans, narrativas simplificadas y contenido memético, más que un entendimiento teórico profundo de la ideología.**

Esta radicalización “rápida pero superficial” contrasta con el proceso adulto, que es “lento pero profundo”. Según los entrevistados tanto de la Policía Nacional como de la Guardia Civil, los adultos típicamente experimentan una radicalización durante un período de seis meses a dos años, un proceso más extendido temporalmente, pero en el que invierten ese tiempo en un consumo cualitativamente diferente: la lectura de manifiestos completos, la visualización de conferencias largas, la participación en debates que requieren

una articulación argumentativa elaborada y el estudio de textos históricos o religiosos que fundamentan la ideología. Cuando el adulto radicalizado es entrevistado, puede articular una cosmología ideológica completa, explicar por qué cree lo que cree, citar autores específicos, responder a contraargumentos y conectar las creencias con experiencias vitales personales.

Esta diferencia tiene implicaciones críticas para la reversibilidad. La radicalización adolescente superficial es frecuentemente más reversible mediante intervenciones relativamente simples (la desconexión del contenido, la exposición a perspectivas alternativas o el desarrollo de un pensamiento crítico básico). La radicalización adulta profunda puede requerir un desmantelamiento ideológico complejo, frecuentemente mediante una terapia prolongada o un programa especializado de desradicalización, porque las creencias se han integrado en la identidad personal de manera que la mera exposición a información contradictoria resulta insuficiente.

Motivaciones primarias - Entretenimiento versus búsqueda de sentido. Los menores, según expertos de la Guardia Civil, “buscan sobre todo entretenimiento, mediante la normalización de la violencia”. La entrada inicial de un adolescente al contenido extremista raramente está motivada por una búsqueda ideológica consciente o una crisis existencial, sino por el consumo de un contenido que es emocionalmente estimulante, transgresor o socialmente gratificante mediante la compartición con pares.

Un menor puede consumir un video de propaganda yihadista mostrando un combate en Siria no porque se adhiera a la yihad como un proyecto político-religioso, sino porque el video tiene:

- Producción cinematográfica profesional (cámara lenta, múltiples ángulos, edición dinámica).
- Banda sonora emocionante (nasheed con vocal potente, percusión intensa).
- Contenido transgresor que proporciona emoción de consumir algo “prohibido” o “peligroso”.
- Valor de shock que genera reacciones fuertes cuando compartido en chat grupal con amigos.

Esta búsqueda de entretenimiento genera una vulnerabilidad específica que no existe en tanta medida con adultos, la normalización gradual de violencia mediante exposición repetida en contexto de consumo hedónico. El adolescente que inicialmente ve el video de combate yihadista y experimenta rechazo visceral (“esto es horrible”), tras visualización de docenas de videos similares durante semanas, experimenta una habituación psicológica donde violencia ya no genera reacción emocional negativa. Esta desensibilización no constituye necesariamente la radicalización ideológica (el menor puede no creer genuinamente que la yihad es obligación religiosa) pero representa la radicalización comportamental donde la violencia se convierte en opción considerada aceptable para resolver conflictos.

Los adultos, en contraste, consumen contenido extremista motivados predominantemente por búsqueda de marcos explicativos que respondan preguntas existenciales o materiales:

- “¿Por qué mi vida es económicamente frustrante pese a la educación universitaria?” → Extrema derecha responde: globalización, inmigración, élites traidoras.
- “¿Por qué experimento alienación social y rechazo romántico?” → Incel responde: determinismo genético, feminismo anti-masculino.
- “¿Cómo puedo recuperar sentido de propósito y comunidad?” → Yihadismo responde: hermandad de creyentes, misión divina, paraíso eterno.

El extremismo proporciona narrativas simplificadas, pero psicológicamente satisfactorias que atribuyen la responsabilidad de sufrimiento personal a causas externas identificables, proporcionando simultáneamente solución (lucha contra enemigo) y comunidad (pertenencia a movimiento). Esta motivación ideológica versus la motivación de entretenimiento explica por qué los adultos frecuentemente demuestran compromiso más profundo y sostenido con el extremismo que los adolescentes, quienes pueden abandonar interés cuando contenido ya no es novedoso o cuando descubren nueva fuente de estimulación.

Plataformas, contenido, y búsqueda de autenticidad. Los menores exhiben comportamiento de consumo disperso y fluido a través de múltiples plataformas mainstream: TikTok para videos virales breves,

Instagram para contenido visual y estético, YouTube para videos medianos (cinco a quince minutos), Discord para chat grupal durante gaming, Snapchat para comunicación efímera con amigos. Esta dispersión refleja menor lealtad a plataformas específicas, mayor susceptibilidad a tendencias virales que migran entre espacios, y consumo predominante de contenido breve (bajo tres minutos) optimizado para atención fragmentada característica de adolescencia digital hiperconectada.

Los adultos, “son más afiliados a buscar contenido original”, según expertos policiales, no generado mediante inteligencia artificial, no reciclado de otras fuentes, no memeficado para su viralización, sino una producción primaria de ideólogos extremistas o documentos históricos auténticos. Esta búsqueda de “autenticidad” se manifiesta en:

- Consumo de manifiestos completos (no extractos): “El gran reemplazo” de Renaud Camus, “Manifiesto” de Anders Breivik, textos de Julius Evola.
- Videos largos de conferencias ideológicas (treinta minutos a tres horas): charlas de Jordan Peterson sobre “marxismo cultural”, conferencias de imanes radicales sobre yihad defensiva.
- Participación en foros de discusión que requieren lectura y escritura extensa: debates teológicos en foros yihadistas, argumentación filosófica en espacios de extrema derecha.
- Desconfianza de contenido “simplificado para masas”: percepción de que memes, clips cortos, son versiones diluidas que no capturan profundidad ideológica.

La plataforma predominante para los adultos radicalizados profundamente es Telegram como un “repositorio de verdad”, percibido como espacio menos censurado que YouTube o Facebook donde pueden acceder a contenido que plataformas mainstream han prohibido. Telegram proporciona sensación de acceder a conocimiento oculto, prohibido, que “sistema” no quiere que las personas conozcan, reforzando la narrativa de ser parte de élite consciente versus masas engañadas.

6. Casos fuera de categorización: la imprevisibilidad de la vulnerabilidad

Más allá de las dos agrupaciones principales descritas, la investigación documentó múltiples casos que desafían cualquier intento de categorización mediante perfiles demográficos, psicológicos, o sociológicos convencionales. Estos casos subrayan una realidad inquietante: la vulnerabilidad a radicalización extrema no se limita a poblaciones fácilmente identificables mediante factores de riesgo tradicionales.

Individuos con educación superior y estabilidad económica. Profesionales con títulos universitarios, empleos estables, ingresos cómodos, que no experimentan declive material ni frustración económica significativa, pero radicalizan mediante exposición a teorías conspirativas, identitarismo cultural, o extremismo presentado como posición intelectual sofisticada. Para estos individuos, el extremismo no responde a privación material sino a necesidad de sentido superior, identidad colectiva trascendente, o simplemente curiosidad intelectual mal dirigida hacia contenido radicalizado presentado con apariencia de rigor.

Mujeres en movimientos explícitamente misóginos. Aunque las comunidades incel son abrumadoramente masculinas por definición ideológica, se documentaron casos de mujeres participando en espacios extremistas misóginos mediante adopción de identidad de “no como otras mujeres”, internalizando misoginia y obteniendo estatus dentro de comunidad mediante validación de narrativas sobre “naturaleza femenina” corrupta de la cual ellas se distancian. Este fenómeno replica dinámicas de minorías que internalizan la opresión y colaboran con la mayoría opresora para obtener una aceptación condicional.

Inmigrantes en movimientos anti-inmigración. Casos documentados evidencian que incluso individuos que serían targets de ideología extrema pueden adoptar esa ideología mediante lógica de “yo soy diferente, yo me integré correctamente, estos otros son el problema”

Funcionan como “tokens”¹⁶ que extremistas utilizan para defenderse de acusaciones de racismo (“no podemos ser racistas, mira, tenemos miembro negro/árabe/latino que está de acuerdo”).

Personas con trauma previo no relacionado. Individuos con historias de abuso, pérdida traumática, enfermedad mental, o crisis existencial que encuentran en extremismo narrativa que da sentido a dolor previamente inexplicable. El extremismo proporciona enemigo externo sobre quien proyectar sufrimiento interno, comunidad que valida dolor, y misión que proporciona propósito donde previamente existía vacío.

Radicalización como experimentación identitaria adolescente. Existen casos en los que el extremismo representa una fase exploratoria propia de la adolescencia, similar a la experimentación con subculturas musicales, estilos visuales o identidades políticas diversas que son adoptadas y posteriormente abandonadas. Para algunos individuos, el extremismo en línea constituye una forma de performance temporal carente de una convicción profunda; sin embargo, el riesgo persiste, ya que una performance prolongada puede transformarse en una creencia genuina mediante un proceso psicológico de internalización.

Radicalización por aburrimiento o trolling. Existen individuos que inician su participación en espacios extremistas motivados por la diversión transgresora, el deseo de provocar reacciones, o simplemente la búsqueda de entretenimiento en ausencia de alternativas más constructivas. La línea entre el “trolling”¹⁷ irónico y la convicción genuina es porosa; muchos nazis contemporáneos comenzaron participando en espacios como 4chan “por las risas” antes de internalizar una ideología que inicialmente reproducen de manera irónica.

16 El término proviene del concepto sociológico de tokenismo (tokenism), el cual describe la práctica de incluir de forma simbólica, superficial o meramente estética a un número muy limitado de personas pertenecientes a un grupo minoritario o discriminado con el único fin de proyectar una imagen de diversidad, inclusión o tolerancia, y así desviar las críticas de discriminación estructural (Alvesson & Billing, 1997). En el ámbito de la radicalización contemporánea, la literatura documenta cómo los grupos de extrema derecha institucionalizada e identitaria instrumentalizan a estos miembros excepcionales como escudos retóricos para blanquear su imagen pública, inmunizarse ante reproches legales y legitimar discursos xenófobos frente a audiencias moderadas.

17 El trolling (troleo) se refiere a la práctica deliberada en comunidades virtuales de publicar mensajes provocadores, irrelevantes o abiertamente ofensivos con el objetivo de generar respuestas emocionales intensas, perturbar el debate normal y desestabilizar la moderación de las plataformas (Sugiura, 2021)

Mujeres en la yihad. El análisis de la participación femenina en espacios yihadistas online durante la última década revela una transformación radical que desafía las narrativas tradicionales sobre mujeres como víctimas pasivas de reclutamiento. Esta evolución desde roles domésticos tradicionales hacia activismo digital agresivo ilustra la adaptación del extremismo religioso a dinámicas de rol de influencia, según expertos de la Policía Nacional.

Durante auge territorial del Estado Islámico (2014-2016) y años inmediatamente posteriores, las mujeres radicalizadas en espacios yihadistas online adoptaban roles que reproducían la estructura patriarcal extrema presentada como ideal religioso. El contenido producido por estas mujeres enfatizaba la identidad de “esposa de muyahidín”: mujer cuya contribución a la yihad es indirecta mediante la construcción de la familia islámica “pura”, crianza de futuros combatientes, y mantenimiento del hogar que permite a esposo dedicarse completamente a lucha armada sin distracciones domésticas.

Esta narrativa glorificaba la domesticidad extrema como forma de resistencia política-religiosa contra el Occidente “corrupto”. El mensaje implícito era que la participación de la mujer en yihad es fundamentalmente diferente de la participación masculina: hombres luchan físicamente, mujeres luchan mediante reproducción biológica y cultural de la próxima generación de yihadistas. Esta división de roles era presentada como complementariedad sagrada ordenada por Dios, no como opresión.

Crucialmente, la reafirmación psicológica que estas mujeres buscaban y obtenían no provenía de audiencia masiva sino de círculo cerrado de comunidad ideológicamente alineada. Una mujer que publicaba fotografía de su cocina con *caption* (descripción a pie de foto en redes) “preparando comida halal para mis siete hijos mientras esposo está en ribat [defensa de frontera islámica]” recibía decenas de comentarios de otras mujeres yihadistas celebrando su “pureza”, “sumisión correcta a voluntad divina”, y contraste favorable con mujeres musulmanas “occidentalizadas” que trabajaban profesionalmente o estudiaban en universidades mixtas.

Después del colapso territorial del Estado Islámico en 2019, cuando las mujeres que habían emigrado a Siria/Iraq fueron capturadas, repatriadas, o quedaron indefinidamente en campos de refugiados (Al-Hol, Al-Roj), una nueva cohorte de mujeres radicalizadas online que nunca viajaron físicamente

adoptó roles cualitativamente diferentes. Estas mujeres, frecuentemente jóvenes (dieciocho a veinticinco años), nativas digitales que crecieron con Instagram y YouTube, reconocieron que la construcción de la audiencia online proporcionaba forma de activismo yihadista más accesible (no requiere emigrar a zona de guerra) y potencialmente más impactante (capacidad de influenciar miles versus influencia limitada a familia nuclear) que roles domésticos tradicionales. Comenzaron a producir contenido propagandístico activamente.

La mecánica es perversamente simple: “en muchos casos, cuanto más contenido potente o polarizador, más seguidores que les reafirman”, afirman expertos del Servicio de Información de Guardia Civil. Esta búsqueda de seguidores crea dinámica de radicalización competitiva entre múltiples mujeres produciendo contenido yihadista que compiten implícitamente por audiencia limitada de usuarios radicalizados o radicalizables. Los seguidores que estas mujeres no son solo audiencia pasiva sino una comunidad activa que proporciona refuerzo psicológico constante mediante la validación de cada post.

Este refuerzo es psicológicamente potente porque satisface necesidades humanas fundamentales de pertenencia grupal, reconocimiento de pares, y sentido de propósito o misión.

Estos casos subrayan una limitación fundamental de perfiles de riesgo. Aunque pueden identificar poblaciones con probabilidad estadísticamente elevada de vulnerabilidad, no pueden predecir casos individuales con certeza, ni pueden identificar exhaustivamente todas las rutas mediante las cuales individuos llegan al extremismo. La radicalización es proceso multicausal, contingente, y frecuentemente impredecible que resiste reducción a fórmulas simples.

7. Síntesis: matriz multidimensional de vulnerabilidad y acumulación de factores de riesgo

La vulnerabilidad a radicalización extremista no constituye una característica binaria simple (presente versus ausente) ni puede determinarse mediante checklist mecánica de factores aislados. Por el contrario, opera como **fenómeno multidimensional complejo que resulta de la intersección**

dinámica de múltiples factores demográficos, psicológicos, sociales, económicos, y tecnológicos que se potencian mutuamente mediante efectos sinérgicos. La presencia de factor único raramente genera vulnerabilidad significativa; es la acumulación progresiva y la interacción entre factores lo que transforma riesgo moderado en vulnerabilidad crítica.

Esta dinámica puede conceptualizarse mediante una matriz multidimensional donde cada eje representa una categoría de factores (demografía, psicología, contexto social y exposición digital) y la vulnerabilidad aumenta exponencialmente, no linealmente, a medida que el individuo acumula factores en múltiples dimensiones simultáneamente. Un varón joven hiperconectado que pasa ocho horas diarias en redes sociales no es necesariamente vulnerable si mantiene una red social presencial sólida, un empleo satisfactorio, unas relaciones afectivas saludables y consume contenido diverso mediante múltiples fuentes con perspectivas variadas. Sin embargo, ese mismo varón joven hiperconectado que además experimenta un aislamiento social profundo (sin amigos cercanos o con una familia distante), más una frustración económica sostenida (un desempleo prolongado o un subempleo crónico que no permite la independencia), más una exposición algorítmica intensiva al contenido extremista (los algoritmos detectan la vulnerabilidad emocional mediante patrones de consumo y recomiendan progresivamente un contenido más radical), ve su vulnerabilidad aumentar no aditivamente, sino exponencialmente mediante efectos de refuerzo mutuo.

El aislamiento social genera un mayor tiempo invertido online buscando conexión, lo cual aumenta la exposición algorítmica. La frustración económica genera una búsqueda de explicaciones que preserven la autoestima, haciendo que las narrativas extremistas que externalizan la culpa resulten psicológicamente atractivas. La exposición repetida al contenido extremista normaliza ideas que inicialmente habrían generado rechazo, reduciendo la resistencia a una radicalización adicional. El proceso se autorrefuerza: cada factor amplifica los efectos de los otros factores, creando una espiral descendente donde la vulnerabilidad genera una mayor exposición al extremismo, que profundiza el aislamiento social mediante el alejamiento de los moderados, lo que aumenta la frustración y la desesperanza e intensifica la búsqueda de sentido en las narrativas extremistas.

Crucialmente, los factores operan mediante umbrales no lineales. Tres factores moderados pueden no generar una vulnerabilidad significativa; pero un cuarto factor, incluso moderado, puede catalizar la transformación hacia una alta vulnerabilidad mediante la superación del umbral crítico. Adicionalmente, ciertos factores actúan como multiplicadores que amplifican dramáticamente los efectos de otros: un trauma previo no procesado multiplica el impacto de las narrativas de victimización; una baja autoestima multiplica la susceptibilidad a las comunidades que ofrecen una validación incondicional; y un pensamiento conspirativo predisposicional multiplica la receptividad a las teorías de gran conspiración.

Esta comprensión de la vulnerabilidad como una matriz multidimensional tiene implicaciones fundamentales para la prevención. Las estrategias efectivas deben operar en múltiples niveles simultáneamente: reducir el aislamiento social mediante el fortalecimiento de vínculos comunitarios presenciales; abordar la frustración económica mediante políticas de empleo juvenil y movilidad social; desarrollar una alfabetización digital crítica que genere resistencia a la manipulación algorítmica; proporcionar apoyo psicológico para el trauma y la salud mental; y regular las plataformas digitales para interrumpir la amplificación algorítmica del extremismo. Una intervención en una dimensión única (por ejemplo, solo educación digital sin abordar el aislamiento social ni la frustración económica) probablemente resultará insuficiente porque los factores en otras dimensiones continuarán generando vulnerabilidad.

Finalmente, la matriz de vulnerabilidad no es estática, sino dinámica: los factores de riesgo fluctúan temporalmente, pueden aparecer o desaparecer mediante cambios vitales (la pérdida de empleo aumenta la vulnerabilidad; un nuevo empleo satisfactorio la reduce; el fin de una relación romántica la aumenta; y una nueva relación saludable la reduce), y la acumulación puede acelerarse o desacelerarse. Esta naturaleza dinámica significa que los individuos pueden transitar entre estados de baja y alta vulnerabilidad múltiples veces durante su trayectoria vital, requiriendo una vigilancia continua y una capacidad de intervención oportuna cuando los factores se acumulan peligrosamente, en lugar de asumir que una evaluación única de vulnerabilidad permanece válida indefinidamente.



PERFILES DE MAYOR VULNERABILIDAD



VARÓN JOVEN HIPERCONECTADO (18-30 años)

Factores de riesgo convergentes:

- Aislamiento social + frustración económica
- Fracaso romántico/sexual [puerta a ideología incel]
- 6-10h diarias online sin vínculos presenciales
- Literacidad técnica sin pensamiento crítico

Señales de alerta:

Lenguaje codificado ["remigración", "blackpill"] · Cambio consumo medios · Estética extremista · Aislamiento progresivo · Expresión abierta de odio

DOBLE VULNERABILIDAD: Online → Offline

La radicalización transita al espacio físico:

- Fight clubs y entrenamientos combate (casos Madrid 2026)
- Centros sociales de extrema derecha
- Hinchadas ultras deportivas como vector reclutamiento
- Eventos y manifestaciones que construyen identidad grupal



ADOLESCENTE EN CRISIS (12-17 años)

Vulnerabilidad crítica:

- 6-10h online como único espacio interacción
- Presión de pares digitalizada (likes, engagement)
- Pensamiento crítico en desarrollo
- Velocidad radicalización acelerada: semanas vs meses

Salud mental:

75% incels con depresión clínica · Normalización ideación suicida en comunidades · Baja autoestima por comparación constante

DOBLE VULNERABILIDAD: Gaming como puerta

90.1% radicalización yihadista España implicó espacios virtuales

- Servidores Discord: gaming → político → extremista
- Chats de voz: lenguaje racista normalizado como "broma"
- Streamers como influencers de radicalización progresiva

Contextos mayor riesgo: Bullying escolar · Exposición temprana sin supervisión · Control parental excesivo o ausente

IMPORTANTE: TODOS LOS PERFILES SON VULNERABLES

Esta investigación documenta radicalización en todos los grupos demográficos: mujeres, adultos mayores, menores de 12 años, todos los niveles educativos y contextos socioeconómicos. Los perfiles destacados concentran el mayor riesgo estadístico, pero ningún grupo es inmune. La prevención debe ser universal con estrategias diferenciadas.

Factores transversales (aplican a TODOS):

- Crisis personal
- Aislamiento social
- Búsqueda significado
- Trauma previo
- Exposición algorítmica sin pensamiento crítico



PROPUESTAS DE INTERVENCIÓN Y RESPUESTA

El análisis exhaustivo del extremismo digital desarrollado en las secciones previas documenta una amenaza compleja, multifacética y en constante evolución que opera mediante una sofisticación técnica considerable y la explotación sistemática de las vulnerabilidades humanas. Sin embargo, la mera documentación del problema resulta insuficiente sin la traducción de los hallazgos en estrategias concretas, realistas y aplicables de prevención, detección temprana, intervención y respuesta institucional coordinada.

Las propuestas que siguen se fundamentan en los modelos de responsabilidad compartida documentados en los informes del EU Knowledge Hub on Prevention of Radicalisation sobre los espacios gaming (2022), GIFCT sobre extremismo y videojuegos (2025), y el TE-SAT de Europol (2025), reconociendo que ningún sector puede abordar unilateralmente el desafío que opera mediante la intersección de la tecnología, la psicología, la educación y las dinámicas sociales.

Estas recomendaciones de prevención y respuesta identifican las áreas prioritarias de actuación basándose en la evidencia empírica recopilada durante la investigación. No constituyen un manual de implementación detallado, sino una hoja de ruta estratégica que señala las direcciones fundamentales hacia las cuales deben orientarse las políticas públicas, las colaboraciones público-privadas y las iniciativas comunitarias. De cara al futuro, **se propone el desarrollo de una Fase II que traduzca estas recomendaciones generales en un manual operativo de buenas prácticas**, el cual incluirá ejercicios específicos, casos prácticos, materiales descargables, protocolos detallados y herramientas concretas adaptadas a los diferentes usuarios (familias, educadores, profesionales de salud mental, plataformas tecnológicas, investigadores y fuerzas de seguridad).

1. Marco regulatorio: expansión legislativa hacia el extremismo multi-ideológico

1.1 El paradigma actual y sus limitaciones

El Reglamento europeo 2021/784, aplicado en España mediante el CITCO y la Unidad Nacional de Retirada de Contenidos Ilícitos de Internet conocida como UNECI, representa un avance significativo en la gobernanza digital del terrorismo. Durante el período 2023-2024, el Centro de Inteligencia

contra el Terrorismo y el Crimen Organizado (CITCO) emitió ciento treinta y cuatro órdenes de retirada que afectaron a miles de materiales distribuidos en plataformas tan diversas como Telegram, Facebook, Instagram, TikTok, Twitter ahora denominado X, SoundCloud, Google Drive, Steam e Internet Archive. De acuerdo con el primer informe de transparencia publicado por la Unidad Nacional de Retirada de Contenidos Ilícitos en Internet (UNECI), el 65% de estas acciones coercitivas estuvo dirigido a dismantelar la propaganda de matriz yihadista, mientras que el 35% restante se aplicó sobre los contenidos vinculados a las ideologías extremistas violentas de carácter racista, xenófobo o ultranacionalista. El plazo máximo establecido de una hora para la eliminación del contenido terrorista tras la notificación oficial constituye una herramienta regulatoria poderosa que España ha implementado activamente mediante UNECI como punto nacional de contacto.

Sin embargo, el marco actual concentra su definición de “contenido terrorista” predominantemente en el yihadismo, reflejando el paradigma histórico donde el terrorismo se equiparaba casi exclusivamente con el extremismo religioso violento de inspiración islamista. Esta investigación documenta empíricamente que el extremismo contemporáneo español y europeo es profundamente multi-ideológico, registrando una creciente presencia en línea de la extrema derecha, la misoginia asociada a la manófera y la extrema izquierda violenta. La coexistencia digital de estos vectores antagonistas activa las dinámicas de radicalización recíproca, un proceso mediante el cual los extremismos de signo opuesto operan como espejos simétricos que se retroalimentan y justifican mutuamente, utilizando la amenaza real o percibida del adversario para acelerar la captación de jóvenes, polarizar las comunidades virtuales y legitimar sus propias agendas de violencia armada (Observatorio Internacional de Estudios sobre Terrorismo, 2025; Pratt & Reidy, 2022). Ninguna de estas corrientes encaja cómodamente en las definiciones tradicionales de “terrorismo” pese a promover una violencia ideológica comparable en intensidad y peligrosidad al yihadismo tradicionalmente monitorizado.

1.2 Ampliación de las categorías punibles: hacia un marco multi-ideológico

La literatura internacional y las recomendaciones de organismos como el EU Knowledge Hub on Prevention of Radicalisation y ICCT sugieren que la modificación legislativa nacional, compatible con el marco europeo existente, debería expandir las categorías de contenido extremista sujeto a las órdenes de retirada más allá del terrorismo stricto sensu. Esta ampliación cubriría áreas identificadas durante la investigación como especialmente problemáticas y actualmente insuficientemente reguladas.

Entre las categorías recomendadas por la literatura especializada se encuentra la glorificación del genocidio histórico, que incluiría la apología explícita del Holocausto, los regímenes totalitarios responsables de los crímenes masivos documentados, o las figuras específicas responsables de los genocidios. El análisis documentó la glorificación sistemática de líderes fascistas mediante canales que utilizan eufemismos para evadir la detección automatizada pero que comunican inequívocamente la apología de los crímenes históricos.

Asimismo, la literatura sugiere abordar las amenazas específicas contra las personas identificables, abarcando el lenguaje eliminacionista dirigido contra los individuos concretos mencionados por su nombre o mediante las características que permiten una identificación inequívoca. La investigación documentó las amenazas directas contra figuras públicas, las campañas coordinadas de acoso y múltiples casos de doxxing donde la información personal sensible fue publicada con la intención maliciosa de facilitar el acoso físico o la violencia directa.

Finalmente, los expertos recomiendan regular la incitación sistemática a la violencia contra los grupos, diferenciada cuidadosamente de la mera expresión de opinión política impopular que permanece protegida constitucionalmente por la libertad de expresión. Esta categoría no penalizaría la crítica política legítima, por vehemente que sea, sino los llamados repetidos y explícitos a la violencia física contra los grupos definidos por las características protegidas como la raza, la religión, la orientación sexual, el género o la nacionalidad.

1.3 Justificación mediante evidencia internacional

Como señala el informe del ICSR titulado “Childhood Innocence? Mapping Trends in Teenage Terrorism Offenders” publicado en 2023, los casos crecientes de menores involucrados en el extremismo violento subrayan la urgencia de revisar y adaptar las políticas de prevención, protección y justicia más allá del paradigma clásico del “terrorista adulto”. La realidad contemporánea documenta a los adolescentes europeos radicalizados mediante múltiples ideologías extremistas, evidenciando la necesidad de marcos regulatorios que aborden el extremismo en su diversidad ideológica contemporánea.

Adicionalmente, como documenta ICCT (2023), la misoginia extrema online debe ser entendida como un componente emergente del paisaje de radicalización digital, ampliando la definición clásica del extremismo y demandando su consideración en el análisis sobre la violencia ideológica contemporánea. La normalización de la ideación suicida en las comunidades incel, documentada extensamente en esta investigación mediante el análisis de Reddit, representa una crisis de salud pública que intersecta con el riesgo de violencia dirigida externamente.

1.4 Regulación de Inteligencia Artificial y contenido sintético

El análisis de ASEAN publicado en 2024 sobre la “espada de doble filo” de la inteligencia artificial en el contexto del extremismo violento pone de relieve la necesidad urgente de desarrollar los marcos normativos, legales y de gobernanza tecnológica que regulen el uso de la IA. Dado que muchas jurisdicciones, incluyendo España, carecen aún de una regulación específica sobre el contenido generado mediante la IA, la literatura advierte del peligro del vacío normativo que facilite la explotación de estas tecnologías por los grupos extremistas para generar la propaganda sintética indistinguible del material auténtico.

Los expertos internacionales recomiendan establecer la obligación del marcaje digital del contenido sintético, donde los videos, las imágenes o el audio generados mediante la IA incluyan marcas digitales verificables que identifiquen inequívocamente el contenido como sintético. La tecnología de marcaje ya existe mediante los sistemas desarrollados por la industria

tecnológica; la regulación requeriría la implementación obligatoria de estos estándares técnicos.

Complementariamente, la literatura sugiere una supervisión reforzada de la financiación mediante las criptomonedas, reconociendo que la evidencia internacional documenta una tendencia creciente de los extremistas utilizando la tecnología blockchain para evadir los sistemas financieros tradicionales (Europol, 2025; King & Meadows, 2024).

Finalmente, los organismos especializados recomiendan el desarrollo de las capacidades técnicas en la moderación automatizada con la supervisión humana obligatoria. Los sistemas de IA pueden detectar preliminarmente el contenido potencialmente extremista, pero la decisión final de eliminación debe incluir una revisión humana que contextualice el contenido y distinga entre el extremismo genuino y los falsos positivos como el periodismo, la investigación académica o la sátira política.

1.5 Salvaguardas contra censura gubernamental

La ampliación de las categorías punibles genera una preocupación legítima, señalada por múltiples organizaciones de derechos civiles, sobre el potencial peligro de la censura de la expresión política lícita mediante las definiciones excesivamente amplias del término “extremismo”. La literatura especializada recomienda incluir mecanismos de apelación independiente que garanticen el control institucional frente al posible abuso gubernamental del marco regulatorio ampliado. Estos mecanismos deberían involucrar a la judicatura especializada en los derechos fundamentales, los representantes de la sociedad civil y los expertos académicos en el análisis del extremismo.

2. Cooperación público-privada con plataformas tecnológicas

2.1 Modelo de responsabilidad compartida

El informe del GIFCT titulado “2024 Resource List: Violent Extremism, Radicalization, and Gaming”, publicado en 2025, representa un esfuerzo concreto de la industria tecnológica y de los actores globales para reconocer que los videojuegos y los espacios denominados “gaming-adjacent” no son

inmunes al riesgo de explotación por parte de los actores extremistas. El documento propone un enfoque de “responsabilidad compartida” donde las plataformas tecnológicas, las empresas de videojuegos, las autoridades, los académicos y la sociedad civil colaboran para implementar las políticas de seguridad, la moderación responsable, la compartición de información sobre contenidos extremistas y el desarrollo de las herramientas de prevención.

Este modelo reconoce que las plataformas no son meros intermediarios neutrales, sino actores con una capacidad técnica considerable y una responsabilidad corporativa de prevenir que su infraestructura sea explotada sistemáticamente por los extremistas. Simultáneamente, el modelo rechaza la delegación total de la responsabilidad a las plataformas, reconociendo que las autoridades públicas mantienen la obligación primaria de la protección de la ciudadanía.

2.2 Expansión de los sistemas de detección automatizada

Esta investigación aboga enfáticamente en que las plataformas tecnológicas expandan sus sistemas de detección automatizada para incorporar lenguaje codificado multi-modal (números como “1515”, emojis politizados como 🦅 (nacionalista), eufemismos como “remigración” o “Gran Reemplazo”, que actualmente evade moderación algorítmica diseñada exclusivamente para detectar términos explícitos. La sofisticación creciente del lenguaje codificado documentada en esta investigación, donde extremistas desarrollan vocabularios completos que comunican significado inequívoco a iniciados mientras permanecen invisibles para algoritmos, exige la evolución correspondiente de las tecnologías de moderación que integren el análisis contextual, reconocimiento de patrones semánticos, y bases de datos actualizadas continuamente de códigos emergentes mediante la colaboración activa con investigadores, fuerzas de seguridad, y comunidades afectadas que identifican nuevos códigos en tiempo real antes de que se generalicen.

La literatura especializada documenta que los sistemas actuales de detección automatizada presentan limitaciones significativas frente al lenguaje codificado que los extremistas desarrollan continuamente (Sugiura, 2021; United Nations Office on Drugs and Crime, 2023) Se recomienda que

las plataformas evolucionen sus tecnologías de moderación incorporando el análisis contextual, el reconocimiento de los patrones semánticos y las bases de datos actualizadas de los códigos emergentes. Esta actualización requiere la colaboración activa entre las plataformas, los investigadores, las fuerzas de seguridad y las comunidades afectadas que pueden identificar los nuevos códigos en tiempo real.

2.3 Hash-Sharing y bases de datos compartidas

El sistema de hash-sharing¹⁸ constituye una herramienta técnica documentada en múltiples informes internacionales como mecanismo efectivo para la prevención de la redistribución del contenido extremista ya identificado. Un *hash* es una huella digital única de un archivo específico que permite su identificación sin necesidad de almacenar o revisar el contenido completo.

La literatura recomienda la implementación de bases de datos compartidas donde las plataformas participantes puedan verificar automáticamente si el contenido que un usuario intenta publicar coincide con material extremista previamente identificado (Global Internet Forum to Counter Terrorism (GIFCT), 2025). Este sistema proporciona una prevención proactiva donde el contenido es bloqueado antes de la publicación, reduciendo significativamente la exposición a la propaganda extremista.

Los expertos reconocen las limitaciones técnicas: los extremistas pueden evadir el sistema mediante modificaciones mínimas de los archivos. Sin embargo, incluso con esta limitación, el hash-sharing aumenta significativamente la fricción y el esfuerzo requerido para la distribución masiva de propaganda, funcionando como una barrera efectiva, aunque no absoluta.

¹⁸ El Hash-Sharing (compartición de hashes) es una técnica de ciberseguridad donde plataformas tecnológicas comparten huellas digitales únicas ("hashes") de archivos, imágenes o videos para identificar y eliminar contenido malicioso, ilegal o terrorista. Actúa como una base de datos colaborativa que permite a las empresas bloquear proactivamente la difusión de material nocivo (GIFCT).

2.4 Iniciativas específicas para espacios gaming

El informe de EU Knowledge Hub on Prevention of Radicalisation (antes RAN) titulado “Countering the Misuse of Gaming-Related Content & Spaces”, publicado en 2022, documenta que la infiltración extremista en la cultura de los videojuegos no refleja una culpabilidad intrínseca de este medio, sino una explotación estratégica de los espacios digitales populares entre los jóvenes. La investigación confirmó la presencia de contenido extremista camuflado en servidores de Discord nominalmente dedicados a los videojuegos, grupos de Steam bajo temáticas históricas, y chats de voz en juegos multijugador.

Este informe propone un modelo de responsabilidad compartida específicamente adaptado al ecosistema de los videojuegos, destacando la necesidad de los enfoques basados en la moderación comunitaria, la colaboración directa con las plataformas de juego y el fortalecimiento de las iniciativas de participación de los jugadores. Las estrategias recomendadas incluyen la implementación de moderación activa en los chats internos de los juegos, el bloqueo de la simbología extremista en los avatares y los sistemas de reporte accesibles que permitan a los jugadores señalar el comportamiento extremista.

La literatura también sugiere el desarrollo de contenidos educativos y narrativas alternativas que promuevan la alfabetización digital y el pensamiento crítico, compitiendo con el extremismo en el mismo terreno cultural que los jóvenes habitan cotidianamente. Las campañas de resiliencia digital adaptadas específicamente a las comunidades de videojuegos pueden distribuir los mensajes de prevención mediante los canales que la audiencia objetiva realmente consume: creadores de contenido populares, youtubers especializados y torneos de deportes electrónicos.

3. Sector educativo: alfabetización digital sin saturación docente

3.1 Integración curricular en asignaturas existentes

La literatura sobre educación preventiva contra el extremismo digital, documentada extensamente por el EU Knowledge Hub on Prevention of Radicalisation, recomienda enfáticamente la integración de la alfabetización digital crítica en las asignaturas existentes versus la creación de nuevas

asignaturas independientes. Esta recomendación responde al reconocimiento de la saturación curricular que enfrentan los sistemas educativos europeos y la necesidad de soluciones implementables sin reestructuraciones masivas.

Los expertos sugieren que la alfabetización digital crítica puede incorporarse naturalmente en múltiples asignaturas: Lengua y Literatura mediante el análisis crítico de los textos digitales contemporáneos (memes, publicaciones en redes sociales, videos virales); Ciencias Sociales mediante el contexto histórico del extremismo y la comparación con los movimientos totalitarios; y Tecnología mediante la comprensión del funcionamiento de los algoritmos de recomendación y las mecánicas de viralización.

El TE-SAT 2025 de Europol advierte que la implicación creciente de los menores y los jóvenes en las conductas extremistas exige reforzar la alfabetización mediática, la educación en el pensamiento crítico y los mecanismos institucionales para detectar las señales tempranas en los entornos digitales.

Los contenidos recomendados por la literatura incluyen: la comprensión de cómo funcionan los algoritmos de recomendación y su tendencia a promover el contenido progresivamente más extremo para maximizar el engagement; las técnicas de verificación de fuentes mediante la triangulación de información desde múltiples fuentes independientes; la identificación de las tácticas de manipulación comunes en la propaganda extremista (simplificación excesiva, creación de enemigos externos, victimización, apelaciones emocionales); y el reconocimiento del lenguaje codificado extremista que permite la comunicación entre los iniciados mientras evade la moderación.

3.2 Detección temprana mediante protocolo para orientadores

La limitación fundamental que debe reconocerse explícitamente es que los docentes no son policías, psicólogos clínicos ni trabajadores sociales especializados. Su rol apropiado en la prevención de la radicalización se limita estrictamente a la detección de las señales de alarma observables en el contexto educativo y a la derivación responsable hacia los profesionales especializados externos. Con esto se evita una intervención directa que excede su competencia profesional y que podría resultar contraproducente mediante una confrontación mal gestionada que profundice la radicalización en lugar de revertirla.

Se enfatiza en que los educadores no deben actuar como investigadores o terapeutas, sino como observadores capacitados que pueden identificar las señales de alarma y derivar los casos hacia los profesionales especializados apropiados.

Los protocolos recomendados incluyen la formación básica de los educadores en el reconocimiento de los indicadores de radicalización, los procedimientos claros de documentación de las observaciones preocupantes, los mecanismos de consulta con los orientadores escolares y los equipos directivos, y los canales establecidos de derivación hacia los servicios externos especializados (salud mental, servicios sociales, fuerzas de seguridad según la gravedad del caso).

4. Herramientas para familias

4.1 Guía familiar práctica de dos páginas

La recomendación principal en términos de prevención familiar del extremismo digital, enfatiza la importancia de mantener canales de comunicación abiertos entre los padres y los hijos adolescentes sobre el consumo digital. Se recomienda evitar tanto la supervisión excesivamente invasiva que destruye la confianza (como la revisión secreta de dispositivos) como la ausencia total de supervisión que permite la exposición no-monitoreada a contenidos extremistas.

Las estrategias recomendadas incluyen la normalización de conversaciones regulares sobre el contenido que los adolescentes consumen online, la visualización ocasional conjunta de videos o contenido como actividad compartida que permite el modelado del pensamiento crítico, y el establecimiento de acuerdos familiares sobre el uso responsable de la tecnología que respeten la privacidad apropiada para la edad mientras mantienen la supervisión parental razonable.

4.2 Identificación de señales de alarma

Se identifican varias señales de alarma que las familias deben reconocer: el uso súbito de lenguaje codificado o referencias que los padres no comprenden, especialmente cuando el adolescente reacciona con hostilidad desproporcionada a preguntas sobre su significado; el aislamiento social progresivo donde el adolescente previamente sociable pasa cada vez más tiempo aislado con dispositivos electrónicos rechazando las actividades familiares o sociales; y la expresión de odio verbal intenso hacia grupos específicos de personas que no había manifestado previamente.

Se enfatiza que estas señales, individualmente o en conjunto, no confirman radicalización, pero justifican atención aumentada y, si persisten, la búsqueda de orientación profesional mediante los orientadores escolares, los psicólogos especializados en adolescentes o los servicios sociales.

5. Profesionales de salud mental: formación especializada accesible

La investigación documentó que los radicalizadores buscan deliberadamente doble vulnerabilidad, identificando jóvenes que ya experimentan crisis de salud mental como depresión clínica, trastornos de conducta alimentaria, ideación suicida activa, o trauma no procesado, quienes son extremadamente receptivos a narrativas extremistas que proporcionan sentido externo a sufrimiento interno y comunidad que valida dolor mediante victimización compartida. Esta intersección entre radicalización y psicopatología exige que profesionales de salud mental incorporen evaluación de riesgo de extremismo en protocolos estándar de evaluación.

Esta intersección, documentada extensamente en la investigación por ejemplo sobre las comunidades incel donde el 75% de los miembros cumplen los criterios de depresión moderada o grave, exige que los profesionales de la salud mental incorporen la evaluación del riesgo de extremismo en sus protocolos estándar de evaluación (Costello et al., 2022).

Se recomienda que los profesionales de la salud mental reciban formación sobre: la epidemiología de la radicalización en las poblaciones clínicas; las técnicas de evaluación que integren preguntas sobre el consumo de contenido extremista sin estigmatizar al paciente; las adaptaciones de

las terapias estándar (como la terapia cognitivo-conductual) que aborden simultáneamente los síntomas de salud mental y las creencias extremistas mediante el cuestionamiento de los patrones cognitivos disfuncionales; y los límites éticos de la confidencialidad cuando el paciente expresa la intención creíble de violencia contra otros.

6. Investigadores: protección institucional

La investigación sobre extremismo y terrorismo online implica riesgos directos y significativos para quienes la llevan a cabo, riesgos que van desde trauma vicario por exposición prolongada a contenido extremadamente perturbador hasta amenazas físicas directas cuando extremistas identifican investigadores monitoreando sus espacios. La ausencia generalizada de protocolos institucionales de cuidado, formación preventiva, o apoyo psicosocial estructurado representa vacío crítico en protección de investigadores académicos españoles.

6.1 Protocolos institucionales recomendados

Se recomienda que las instituciones académicas implementen protocolos éticos obligatorios cuando autorizan la investigación sobre el extremismo, incluyendo: la evaluación formal del riesgo previa al inicio de la investigación; la formación obligatoria en la seguridad digital y el autocuidado; la rotación de las tareas para limitar la exposición individual al contenido más perturbador; el acceso garantizado al apoyo psicológico profesional sin estigma; y las colaboraciones formales con las fuerzas de seguridad para la protección física cuando emergen las amenazas.

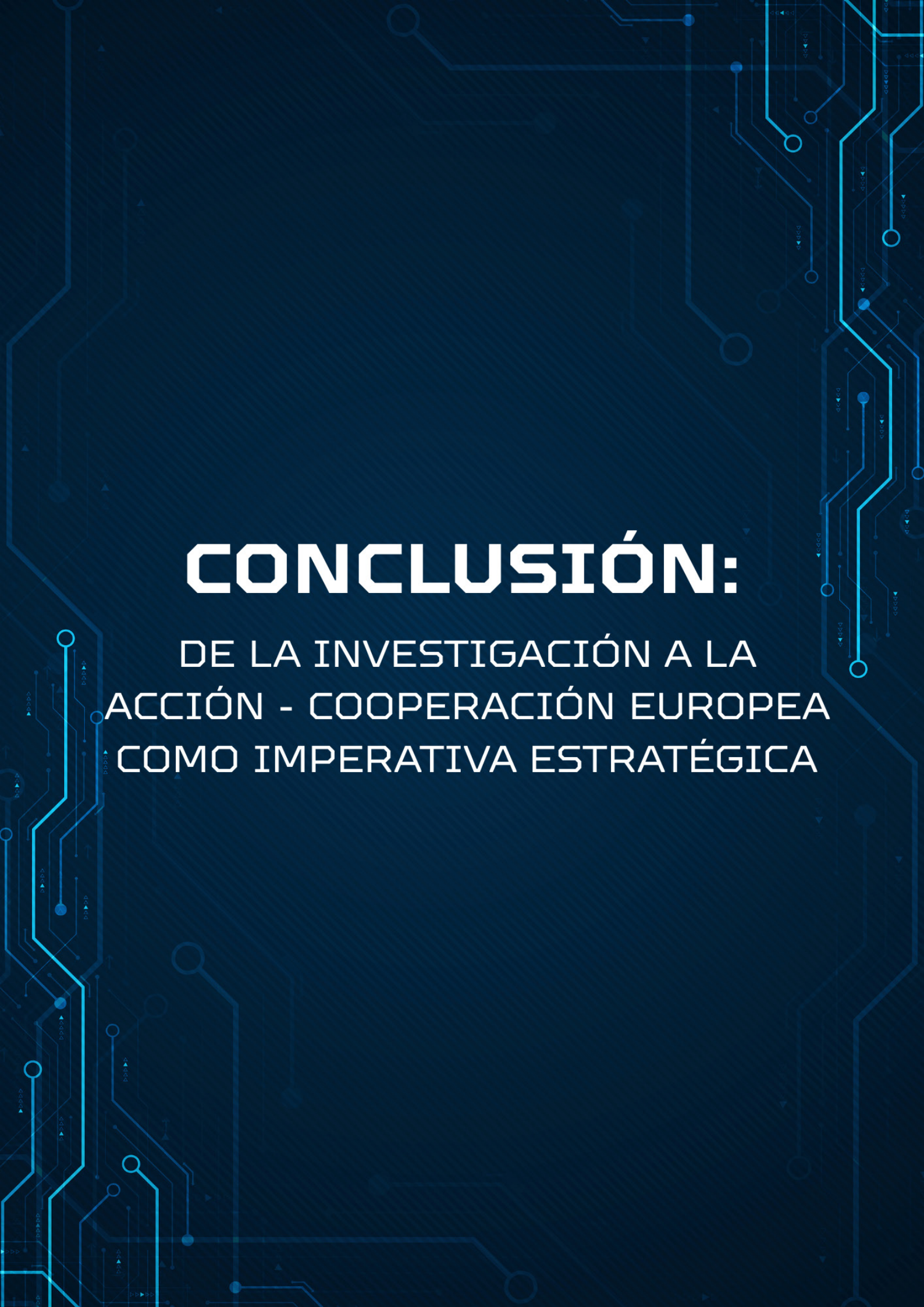
7. Implementación gradual y evaluación continua

7.1 Priorización realista de las intervenciones

La literatura sobre la implementación de las políticas preventivas contra el extremismo enfatiza la necesidad de la priorización cuidadosa y el despliegue gradual que reconozca las limitaciones presupuestarias y la capacidad institucional finita. Los expertos recomiendan comenzar con las intervenciones que presentan el mejor balance entre la viabilidad de implementación y el impacto potencial, expandiendo progresivamente hacia las iniciativas más complejas a medida que se construye la capacidad institucional.

7.2 Evaluación de impacto basada en evidencia

Los organismos especializados subrayan que la evaluación continua del impacto es absolutamente esencial para el refinamiento basado en la evidencia versus la perpetuación de los programas inefectivos por inercia institucional. Las métricas recomendadas incluyen: la evolución documentada de la prevalencia del contenido extremista medida mediante el muestreo sistemático; la proporción de los casos de radicalización detectados tempranamente versus los casos que llegan a la consumación de violencia sin detección previa; y la efectividad de las campañas de contra-narrativa medida mediante los estudios que evalúan los cambios en las actitudes de las audiencias objetivo.



CONCLUSIÓN:

DE LA INVESTIGACIÓN A LA
ACCIÓN - COOPERACIÓN EUROPEA
COMO IMPERATIVA ESTRATÉGICA

Esta investigación ha documentado exhaustivamente la magnitud, la complejidad y la urgencia del desafío que representa el extremismo violento en los entornos digitales europeos. El análisis de miles de contenidos extremistas distribuidos en nueve plataformas principales, complementado con las entrevistas a los especialistas de las fuerzas y cuerpos de seguridad y los expertos en materia de prevención, revela un ecosistema de radicalización profundamente sofisticado, en rápida evolución y fundamentalmente transnacional que no reconoce las fronteras nacionales ni puede ser abordado efectivamente mediante las respuestas fragmentadas o unilaterales.

El estudio identifica doce señales de alarma de máxima gravedad que requieren la atención prioritaria inmediata de las autoridades, las plataformas tecnológicas, el sector educativo y la sociedad civil.

Entre estas, cinco patrones presentan un nivel de riesgo crítico que justifica la movilización de los recursos extraordinarios:

- 1) La glorificación sistemática de violencia histórica (celebraciones de cumpleaños de Hitler, conmemoraciones de quema de libros nazis, santificación de terroristas como Elliot Rodger y Anders Breivik) no constituye una mera expresión política protegida por la libertad de expresión sino una normalización deliberada de atrocidades que reduce inhibiciones morales y puede inspirar imitación directa, como evidencian casos documentados de atacantes que consumieron extensivamente este contenido antes de perpetrar violencia.
- 2) Las amenazas específicas dirigidas a personas identificadas (deportistas, políticos, activistas nombrados con intención intimidatoria, publicación de direcciones y rutinas personales) representan una escalada desde odio abstracto hacia la planificación operativa concreta que históricamente ha precedido violencia física y que crea el clima de intimidación que silencia voces críticas a través del miedo.
- 3) El lenguaje eliminacionista generalizado (“remigración”, “Gran Reemplazo”, “invasión”, referencias a deportación masiva de poblaciones enteras) cumple una función preparatoria que normaliza progresivamente la idea de que determinados grupos humanos no deben o no pueden estar presentes en Europa, creando clima ideológico

que facilita aceptación de medidas cada vez más radicales y que históricamente ha precedido genocidios y limpiezas étnicas.

4) La ideación suicida normalizada documentada especialmente en comunidades incel, donde aproximadamente el setenta y cinco por ciento (75%) de miembros cumplen criterios de depresión moderada o grave y donde el suicidio es discutido como una opción racional mediante términos como “rope” (ahorcamiento) y presentado como una alternativa comprensible a una existencia considerada sin valor, representa una crisis de salud pública de gravedad extrema con implicaciones inmediatas que trascienden seguridad para constituir emergencia sanitaria.

5) La convergencia de múltiples odios en discursos y actores únicos (racismo + antisemitismo + misoginia + homofobia + islamofobia operando simultáneamente) indica no solo un prejuicio aislado sino la adopción de una cosmovisión ideológica completa que distingue la radicalización profunda de opinión política meramente impopular, aumenta probabilidad de violencia mediante multiplicación de targets potenciales, y reduce significativamente probabilidad de persuasión o desradicalización exitosa.

En cuanto a los perfiles de vulnerabilidad, **el análisis identifica dos perfiles de vulnerabilidad que concentran riesgo de radicalización de manera desproporcionada y que deben ser foco prioritario de intervenciones preventivas.**

Por un lado, el varón joven (dieciocho a treinta y cinco años) socialmente aislado, con educación secundaria o universitaria que experimenta fracaso en múltiples dominios vitales simultáneamente (laboral, romántico, social), representa un perfil clásico documentado en casos de radicalización violenta. Este perfil no refleja una patología individual sino una vulnerabilidad estructural generada por la combinación de factores socioeconómicos (precarización laboral, crisis de vivienda, estancamiento de movilidad social ascendente) con factores psicosociales (erosión de estructuras comunitarias tradicionales, aislamiento social creciente en sociedades hiperindividualizadas, crisis de masculinidad en contexto de transformación de roles de género) que el extremismo explota sistemáticamente mediante narrativas de victimización y promesas de restauración de estatus perdido.

Por otro, el adolescente de doce a diecisiete años en crisis de identidad hiperconectado representa un perfil especialmente preocupante por dos razones críticas que justifican su priorización máxima: primero, constituye un segmento demográfico de más rápido crecimiento en casos de radicalización documentados, evidenciando una tendencia alarmante de rejuvenecimiento del extremismo violento que anteriormente afectaba predominantemente a adultos jóvenes; segundo, la condición de menores de edad genera complejidades legales donde los sistemas de justicia juvenil europeos diseñados para delincuencia común carecen de marcos apropiados para abordar la radicalización ideológica y planificación de terrorismo, creando un vacío entre gravedad de amenaza y capacidad institucional de respuesta que respete simultáneamente derechos del menor y seguridad pública. La velocidad de la radicalización adolescente (semanas vs meses en adultos) combinada con la impulsividad característica de desarrollo neurológico incompleto aumenta el riesgo de transición rápida desde consumo de contenido extremista hacia acción violenta sin periodo prolongado de planificación que permitiría detección e intervención.

Respecto a las tácticas de radicalización que explotan vulnerabilidades psicológicas, **la investigación documenta doce tácticas recurrentes empleadas por actores extremistas para captar, adoctrinar, y movilizar audiencias vulnerables** mediante explotación sistemática de necesidades humanas fundamentales (pertenencia, reconocimiento, propósito, coherencia narrativa) y vulnerabilidades psicológicas específicas (aislamiento social, frustración económica, crisis de identidad, necesidad de significado existencial).

Entre estas tácticas, cuatro presentan efectividad particularmente alta que exige respuesta prioritaria: los memes como formato dominante (representando aproximadamente formato más frecuente documentado) que reducen la resistencia psicológica mediante humor mientras normalizan progresivamente contenido extremo mediante la exposición repetida; las comunidades cerradas en Telegram, Discord, y espacios privados donde radicalización ocurre sin moderación externa ni exposición a perspectivas disidentes, permitiendo la escalada competitiva hacia el extremismo mediante una dinámica donde miembros compiten por demostrar mayor compromiso ideológico; la presencia multiplataforma coordinada que proporciona una redundancia contra moderación y especialización funcional

donde TikTok capta mediante videos virales, Instagram amplifica, Telegram adoctrina sin moderación, y Discord coordina planificación operativa; y el lenguaje codificado sofisticado (“remigración”, “1488”, “Gran Reemplazo”, emojis politizados como 🖐️ yihadista) que permite expresión de contenido extremo evadiendo detección automatizada mediante vocabulario técnico o eufemístico que algoritmos no reconocen como extremista.

De las recomendaciones generales hacia la implementación concreta: Propuesta de Fase II

Las propuestas presentadas en esta sección constituyen recomendaciones estratégicas fundamentadas en la literatura internacional y los hallazgos empíricos de esta investigación. Sin embargo, **la traducción efectiva de estas recomendaciones en cambios tangibles sobre el terreno requiere el desarrollo de herramientas operativas específicas, protocolos detallados, materiales pedagógicos y casos prácticos que guíen la implementación concreta.**

Se propone el desarrollo de una Fase II dedicada al diseño de un manual operativo de buenas prácticas que traduzca las recomendaciones generales aquí presentadas en instrumentos directamente utilizables por los diferentes actores:

- **Para las familias:** guías visuales descargables con las señales de alarma específicas ilustradas mediante ejemplos concretos, scripts de conversación para abordar los temas sensibles con los adolescentes, configuraciones técnicas paso a paso de los controles parentales en las plataformas más utilizadas, y directorios de recursos de ayuda accesibles localmente.
- **Para los educadores:** unidades didácticas completas con los planes de lección detallados, los ejercicios prácticos, las rúbricas de evaluación, los protocolos de detección temprana con los formularios de documentación, y los árboles de decisión para la derivación apropiada de los casos según la gravedad.
- **Para los profesionales de la salud mental:** módulos de formación con los casos clínicos ilustrativos, las herramientas de

evaluación validadas, las adaptaciones específicas de los protocolos terapéuticos estándar, y las guías para la navegación de los dilemas éticos sobre la confidencialidad.

- **Para las plataformas tecnológicas:** los catálogos actualizados del lenguaje codificado emergente, las taxonomías de las tácticas extremistas documentadas, los protocolos de colaboración con las autoridades que balanceen la privacidad del usuario con la seguridad pública, y las mejores prácticas de moderación comunitaria.
- **Para los investigadores:** los protocolos de seguridad digital detallados, las listas de verificación de evaluación del riesgo, los recursos de autocuidado estructurados, y los modelos de colaboración institucional con las fuerzas de seguridad.
- **Para las fuerzas y cuerpos de seguridad:** las guías de análisis de las tendencias emergentes, los indicadores de riesgo validados empíricamente, los protocolos de intervención temprana que respeten los derechos fundamentales, y los modelos de colaboración multi-agencia.

Este manual operativo incluiría ejercicios interactivos, simulaciones de casos, materiales audiovisuales, plantillas descargables y personalizables, y un repositorio digital actualizado continuamente que refleje la evolución constante del extremismo digital. **La Fase II convertiría las recomendaciones estratégicas de la investigación actual en una caja de herramientas práctica, accesible y adaptable** que empodere a los diferentes actores para implementar la prevención basada en la evidencia en sus contextos específicos.

No existe un actor único capaz de resolver el extremismo digital unilateralmente mediante la acción aislada nacional. La naturaleza fundamentalmente transnacional del fenómeno (el contenido producido en un país consumido instantáneamente en toda Europa, los reclutadores operando desde las jurisdicciones no-cooperativas, el financiamiento mediante las criptomonedas que evade los controles nacionales, las plataformas tecnológicas con sede fuera de la jurisdicción europea) exige la respuesta coordinada europea que ningún Estado miembro puede implementar efectivamente de manera independiente.

España debe fortalecer sustancialmente su participación activa en las redes europeas especializadas Radicalisation Awareness Network, Europol, EU Internet Forum transitando desde un rol ocasionalmente consultivo hacia un liderazgo proactivo que comparte los hallazgos de las investigaciones como la presente y se beneficia simultáneamente del conocimiento generado en otros Estados miembros, reconociendo que el extremismo detectado en las plataformas españolas frecuentemente tiene el origen en la producción del contenido en otros países europeos, y que el extremismo producido en España se viraliza hacia el resto del continente.

Las funciones centrales de la coordinación europea recomendadas por la literatura incluyen: el intercambio sistemático de las mejores prácticas documentadas entre los países; el sistema de alertas tempranas sobre las tendencias extremistas emergentes detectadas en un país que pueden expandirse a otros; la coordinación de las campañas de contra-narrativa transnacionales producidas simultáneamente en múltiples idiomas; el desarrollo colaborativo de los recursos educativos multilingües que reduzcan los costes mediante la compartición; y la armonización gradual de los marcos legales reconociendo que las asimetrías regulatorias actuales permiten a los extremistas explotar las jurisdicciones con la regulación más laxa como bases de operación.

El coste de continuar con el enfoque fragmentado actual, medido honestamente en las múltiples dimensiones, excede inconmensurablemente la inversión requerida para la implementación coordinada y sostenida de las propuestas desarrolladas en esta investigación y en el futuro manual operativo de la Fase II.

En términos de las vidas humanas, cada ataque terrorista exitoso que la prevención adecuada habría evitado representa no solo las víctimas fatales directas sino las familias destruidas, las comunidades traumatizadas y los ciclos de venganza que perpetúan la violencia generacionalmente. En términos de la salud mental, los miles de jóvenes europeos actualmente inmersos en las comunidades extremistas online experimentan el deterioro psicológico severo que frecuentemente es irreversible si la intervención no ocurre durante la ventana crítica de la adolescencia y la adultez joven temprana. En términos de la cohesión social, la polarización extrema alimentada sistemáticamente por el contenido extremista viralizado sin

obstáculo erosiona la confianza interpersonal, la solidaridad comunitaria y la capacidad de las sociedades democráticas de resolver los conflictos mediante la deliberación y el compromiso en lugar de la confrontación y la violencia.

En términos económicos, el coste de la respuesta reactiva post-ataque (la investigación forense, los juicios, el encarcelamiento de los perpetradores, la compensación a las víctimas, el refuerzo de la seguridad física) supera masivamente la inversión en la prevención que habría evitado el ataque completamente. En términos políticos, cada ataque exitoso fortalece las narrativas autoritarias que presentan la seguridad y la libertad como mutuamente excluyentes, impulsando las restricciones de los derechos civiles que erosionan los fundamentos de la democracia liberal que el extremismo busca destruir.

La pregunta no es si España y Europa pueden permitirse invertir los recursos significativos en la prevención integral del extremismo digital mediante la implementación coordinada de las propuestas desarrolladas en este estudio y su posterior traducción operativa en la Fase II, sino si pueden permitirse continuar con el enfoque fragmentado, sub-financiado y nacional-aislacionista actual que deja los vacíos críticos donde la radicalización florece sin obstáculo, permitiendo que una generación entera de jóvenes europeos sea expuesta diariamente a la propaganda extremista sin la alfabetización digital que les permita resistir la manipulación, sin la supervisión familiar efectiva que detecte las señales tempranas, sin los protocolos educativos que activen la intervención cuando la radicalización es aún reversible, y sin la coordinación europea que reconozca que la amenaza es transnacional y exige la respuesta transnacional proporcionalmente coordinada.

El extremismo digital no es un problema futuro hipotético sino una crisis contemporánea documentada exhaustivamente en los miles de contenidos analizados durante esta investigación. La respuesta no puede ser gradual, experimental o limitada a programas piloto limitados financieramente. Debe ser inmediata, comprehensiva, coordinada multi-actor y sostenida trans-generacionalmente. Las recomendaciones de prevención y respuesta desarrolladas en esta sección proporcionan una hoja de ruta estratégica basada en la evidencia. **La Fase II propuesta traducirá esta hoja de ruta en un manual operativo con las herramientas concretas, los protocolos detallados y los casos prácticos que empoderarán la implementación**

efectiva. La voluntad política, la inversión institucional y el reconocimiento colectivo de que la prevención del extremismo digital es una inversión en el futuro de la democracia europea, la cohesión social y el bienestar de las próximas generaciones determinarán si estas recomendaciones basadas en la evidencia se traducen en los cambios tangibles que la urgencia de la amenaza demanda.



BIBLIOGRAFÍA

Agencia EFE. (2025, 12 de septiembre). *España lidera en Europa la retirada de propaganda terrorista en videojuegos*. <https://efe.com/espana/2026-01-06/videojuegos-propaganda-terrorista-espana/>

Akram, M., & Nasar, A. (2023). Systematic Review of Radicalization through Social Media. *Ege Academic Review*, 23(2), 279–296. <https://doi.org/10.21121/eab.1166627>

Alvesson, M., & Billing, Y. D. (1997). *Understanding gender and organizations*. SCIRP. <https://www.scirp.org/reference/referencespapers?referenceid=2267565>

Balci, U., Sirivianos, M., & Blackburn, J. (2023). *Roll in the Tanks! Measuring left-wing extremism on Reddit at scale*. arXiv. <https://arxiv.org/abs/2307.06981>

BBC News. (2025, 17 de noviembre). *Far-right paramilitary group 'The Base' operating internationally*. The Guardian.

<https://www.theguardian.com/world/2025/nov/17/far-right-paramilitary-the-base>

Binder, J. F., & Kenyon, J. (2022). Terrorism and the Internet: How Dangerous Is Online Radicalization? *Frontiers in Psychology*, 13, 997390. <https://doi.org/10.3389/fpsyg.2022.997390>

CBC News. (2025). *MMA gym owners, coaches ID'd at secretive neo-Nazi event in B.C.* CBC. <https://www.cbc.ca/news/canada/white-supremacist-conference-vancouver-9.6970604>

Centro de Inteligencia contra el Terrorismo y el Crimen Organizado (CITCO). (2025). *Informe de transparencia 2023-2024: Unidad Nacional de Retirada de Contenidos Ilícitos en Internet (UNEI)*. Ministerio del Interior, Gobierno de España. https://www.interior.gob.es/opencms/export/sites/default/.galleries/galeria-de-prensa/documentos-y-multimedia/balances-e-informes/2024/Informe_Retirada_Contenidos_Terroristas_CITCO.pdf

Cinelli, M., De Francisci Morales, G., Galeazzi, A., Quattrociocchi, W., & Starnini, M. (2021). The echo chamber effect on social media. *Proceedings of the National Academy of Sciences*, 118(9), e2023301118. <https://doi.org/10.1073/pnas.2023301118>

Cherney, A., et al. (2022). A Systematic Evidence Review of Rehabilitation Strategies for Young People Involved in Violent Extremism. University of Queensland.

Clifford, B. (2018). Radicalization in Custody: Towards Data-Driven Terrorism Prevention in the United States Federal Correctional System. Program on Extremism, George Washington University.

CNN en Español. (2025, 16 de diciembre). *Clubes de pelea y entrenamiento secreto: CNN localiza el campamento oculto de un grupo supremacista*. CNN. <https://cnnespanol.cnn.com/2025/12/16/eeuu/video/blancos-supremacismo-grupos-lucha-trax>

CNN International. (2026, 31 de enero). *Amelia meme and AI fuel far-right movements*. CNN. <https://edition.cnn.com/2026/01/31/uk/amelia-meme-ai-far-right-intl-scli>

Comisión Europea. (2024, 18 de junio). *Commission launches new EU Knowledge Hub on Prevention of Radicalisation*. https://home-affairs.ec.europa.eu/news/commission-launches-new-eu-knowledge-hub-prevention-radicalisation-2024-06-18_en

Costello, W., Rolón, V., Thomas, A. G., & Buss, D. M. (2022). Levels of well-being among men who are incel (involuntarily celibate). *Research Gate*. https://www.researchgate.net/publication/363484489_Levels_of_Well-Being_Among_Men_Who_Are_Incel_Involuntarily_Celibate

Crónica Global. (2025, 25 de noviembre). *Dentro de la red 'incel' catalana: "Usan el chat de los videojuegos para radicalizar adolescentes"*. Crónica Global. https://cronicaglobal.elespanol.com/vida/20251125/dentro-incel-catalana-usan-videojuegos-radicalizar-adolescentes/1003742710414_0.html

San Juan, N. (2026, 4 de febrero). *El cofundador de Telegram critica la regulación de Sánchez de las redes y el Gobierno señala que es una medida urgente*. <https://www.rtve.es/noticias/20260204/cofundador-telegram-responde-a-sanchez-por-limite-edad-redes-sociales/16923831.shtml>

El Diario. (2025a). *Agencias de inteligencia de Occidente siguen la pista de clubes de lucha neofascistas con lazos internacionales*. El Diario. https://www.eldiario.es/internacional/theguardian/agencias-inteligencia-occidente-siguen-pista-clubes-lucha-neofascistas-lazos-internacionales_1_12728556.amp.html

El Diario. (2025b). *Atomwaffen Division: el grupo neonazi que pretendía instalarse y pasar a la acción en España*. El Diario. https://www.eldiario.es/catalunya/atomwaffen-division-grupo-neonazi-pretendia-instalarse-pasar-accion-espana_1_12869109.html

El País. (2025, 7 de diciembre). *Así se montó la célula supremacista blanca en el triángulo de la cerámica de Castellón: "David siempre ha sido un flipado de las armas, pero nadie pensaba que iba a llegar a tanto"*. El País. <https://elpais.com/espana/2025-12-07/asi-se-monto-la-celula-supremacista-blanca-en-el-triangulo-de-la-ceramica-de-castellon-david-siempre-ha-sido-un-flipado-de-las-armas-pero-nadie-pensaba-que-iba-a-llegar-a-tanto.html>

El Periódico. (2025, 8 de abril). *"Muchos chavales sienten que lo realmente contracultural es ser facha": el impacto de la 'manosfera' en las aulas catalanas*. El Periódico. <https://www.elperiodico.com/es/sociedad/20250408/adolescencia-netflix-impacto-incel-manosfera-aulas-cataluna-machismo-116009671>

European Institute for Gender Equality (EIGE). (2022). *Combating Cyber Violence against Women and Girls*. https://eige.europa.eu/sites/default/files/documents/combating_cyber_violence_against_women_and_girls.pdf

Europol. (2024). *Referral Action Days: Disrupting terrorist and violent extremist content online*. European Counter Terrorism Centre. <https://www.europol.europa.eu/>

Europol. (2025a). *European Union Terrorism Situation & Trend Report 2025 (TE-SAT 2025)*. Europol. https://www.europol.europa.eu/cms/sites/default/files/documents/EU_TE-SAT_2025.pdf

Europol. (2025b). *Europol threat assessment 2025: Violent extremism and terrorism in the EU*. Publications Office of the European Union. <https://www.europol.europa.eu/>

Europol. (2025c). *EU Terrorism Situation and Trend Report (TE-SAT 2025)*. https://www.europol.europa.eu/cms/sites/default/files/documents/EU_TE-SAT_2025.pdf

Facultad de Ciencias Exactas y Naturales, Universidad de Buenos Aires. (2024, 30 de agosto). *¿De qué hablamos cuando hablamos de incels?*. GenEx. <https://exactas.uba.ar/genex/2024/08/30/aproximacion-incels/>

Francia, Gobierno de. (2025). *Francia prohíbe la entrada de 10 activistas de extrema derecha*. Yahoo Noticias. <https://es-us.noticias.yahoo.com/francia-proh%C3%ADbe-entrada-10-activistas-124248397.html>

García-Calvo, C. (2024a). *Evolución de los patrones de radicalización en España: entornos virtuales vs. físicos*. Real Instituto Elcano. <https://www.realinstitutoelcano.org/>

García-Calvo, C. (2024b). *La metamorfosis digital de la captación terrorista: Del entorno físico a los videojuegos*. Real Instituto Elcano. <https://www.realinstitutoelcano.org/>

Global Internet Forum to Counter Terrorism (GIFCT). (s.f.). *What is the Hash Sharing Database?* [Preguntas frecuentes]. <https://gifct.org/?faqs=what-is-the-hash-sharing-database>

Global Internet Forum to Counter Terrorism (GIFCT). (2025a). *2024 Resource List: Violent Extremism, Radicalization, and Gaming*. <https://gifct.org/wp-content/uploads/2025/02/GIFCT-25WG-0225-EG-Resources-1.1.pdf>

Global Internet Forum to Counter Terrorism (GIFCT). (2025b). *Threat surfaces in games: Challenges and best practices*. <https://gifct.org/wp-content/uploads/2025/02/GIFCT-25WG-0225-Threat-Surfaces-1.1.pdf>

Global Internet Forum to Counter Terrorism (GIFCT). (2025c). *Artificial Intelligence: Threats, opportunities, and policy frameworks for countering VNSAs*. https://gifct.org/wp-content/uploads/2025/04/GIFCT-25WG-0425-AI_Report-Web-1.1.pdf

Global Internet Forum to Counter Terrorism (GIFCT). (2025d). *2024 Annual and Transparency Report*. <https://gifct.org/wp-content/uploads/2025/07/GIFCT-Annual-and-Transparency-Report-2024.pdf>

Hedayah. (2023). *Exploring trends and research in countering and preventing extremism & violent extremism*. <https://hedayah.com/app/uploads/2023/11/Exploring-trends-and-research.pdf>

Hoffman, B., Ware, J., & Shapiro, E. (2020). Assessing the threat of incel violence. *St. Andrew Research Repository*. <https://research-repository.st-andrews.ac.uk/handle/10023/24162>

King, M., & Meadows, S. (2024). Crypto-extremism: Tracing the utilization of decentralized finance and blockchain technology by violent far-right and jihadi networks. *Studies in Conflict & Terrorism*, 47(2), 112–134. <https://doi.org/10.1080/1057610X.2024.2301234>

Koch, A. (2024, 15 de abril). *Aligning prayers and push-ups: Exploring the rise of "salafitness"*. Hudson Institute. <https://www.hudson.org/religious-freedom/aligning-prayers-push-ups-exploring-rise-salafitness>

Koch, A., Nahon, K., & Moghadam, A. (2023). White jihad: How white supremacists adopt jihadi narratives, aesthetics, and tactics. *Ideas*. <https://ideas.repec.org/a/taf/ftpvxx/v36y2024i7p919-943.html>

Lamphere-Englund, G. (2025). *Protecting children in online gaming: Mitigating risks from organized violence*. UNICEF Innocenti Working Paper. <https://www.unicef.org/innocenti/media/11836/file/UNICEF-Innocenti-Protecting-Children-Online-Gaming-Working-Paper-2025.pdf>

Milmo, D. (2026, 8 de enero). *Google and Character.AI settle lawsuit with mother of teen who killed himself*. The Guardian. <https://www.theguardian.com/technology/2026/jan/08/google-character-ai-settlement-teen-suicide>

Moreno, F. J. (2024, 21 de marzo). *La "yihad blanca" gana terreno: así opera el aceleracionismo neonazi que preocupa a los servicios de inteligencia*. Escudo Digital. <https://www.escudodigital.com/expertos/opinion/la-yihad-blanca-gana-terreno-asi-opera-el-aceleracionismo-neonazi-que-preocupa-a-los-servicios-de-inteligencia.html>

Neumann, P. R. (2010). *Prisons and Terrorism: Radicalisation and De-radicalisation in 15 Countries*. International Centre for the Study of Radicalisation and Political Violence (ICSR), King's College London.

Observatorio Internacional de Estudios sobre Terrorismo. (2025). *Anuario del terrorismo yihadista 2024*. Colectivo de Víctimas del Terrorismo (COVITE). <https://observatorioterrorismo.com/actividades/anuario-del-terrorismo-yihadista-2024/>

Observatorio Internacional de Estudios sobre Terrorismo. (2026). *Anuario del terrorismo yihadista 2025*. Colectivo de Víctimas del Terrorismo (COVITE). <https://observatorioterrorismo.com/actividades/anuario-del-terrorismo-yihadista-2025/>

Organización Mundial de la Salud. (2024). *Uso de medios digitales y salud mental en adolescentes de la Región Europea de la OMS*. Oficina Regional para Europa de la OMS.

Organisation for Security and Co-operation in Europe (OSCE). (2019). *Understanding the role of gender in preventing and countering violent extremism and radicalization that lead to terrorism*. https://www.osce.org/files/f/documents/0/b/420563_1.pdf

Pérez-García, D., Barragán, L. (2025). La metamorfosis digital de la propaganda yihadista: El uso de plataformas de metaverso y videojuegos infantiles como vectores de radicalización. *Revista Internacional de Estudios sobre Terrorismo (RIET)*, (13), Art. 3. <https://www.rietjournal.org/>

Pearson, E., Whittaker, J., Conway, M., Baaken, T., Zeiger, S., & Atamuradov, F. (2023). *Online Extremism and Terrorism Researchers' Security, Safety, and Resilience: Findings from the Field*. VOX-Pol. <https://voxpath.eu/wp-content/uploads/2024/01/Online-Extremism-and-Terrorism-Researchers-Security-Safety-Resilience.pdf>

Perliger, A., Stevens, C., & Leidig, E. (2023). *Mapping the ideological landscape of extreme misogyny*. ICCT / Asser Institute. <https://icct.nl/sites/default/files/2023-01/Mapping-the-Ideological-Landscape-of-Misogyny%20%282%29.pdf>

Psicología y Mente. (s.f.). *Efecto de homogeneidad relativa del exogrupo: qué es y cómo nos afecta*. <https://psicologiaymente.com/social/efecto-homogeneidad-relativa-exogrupo>

Radicalisation Awareness Network (RAN). (2026, 10 de marzo). *This Is Not a Game: How Steam Harbors Extremists*. EU Knowledge Hub on Prevention of Radicalisation. <https://home-affairs.ec.europa.eu/>

Radio Televisión Española. (2026, 7 de marzo). *Detenidos en Madrid y enviados a prisión dos expertos en artes marciales mixtas vinculados al terrorismo yihadista*. RTVE.es. <https://www.rtve.es/noticias/20260307/detenidos-madrid-enviados-a-prision-dos-expertos-artes-marciales-mixtas-vinculados-terrorismo-yihadista/16969790.shtml>

Ronco, D., Sbraccia, A., & Torrente, G. (2019). Prison De-radicalization Strategies, Programs and Risk Assessment Tools in Europe. European Prison Observatory / Antigone Edizioni.

Rose, H., & Vale, G. (2023). *Childhood Innocence?: Mapping Trends in Teenage Terrorism Offenders*. International Centre for the Study of Radicalisation. <https://icsr.info/wp-content/uploads/2023/11/ICSR-Report-Childhood-Innocence-Mapping-Trends-in-Teenage-Terrorism-Offenders.pdf>

RSIS. (2025, octubre). *Far-Right Extremism and Gaming: How Hate Hijacks Play*. S. Rajaratnam School of International Studies. <https://rsis.edu.sg/rsis-publication/rsis/far-right-extremism-and-gaming-how-hate-hijacks-play/>

Sainz-Pardo, M. (2024, 10 de febrero). *Las narrativas de la persecución: Del victimismo digital a la radicalización en redes*. El Mundo. <https://www.elmundo.es/>

Schlegel, L. (2022). *Countering the misuse of gaming-related content & spaces: Inspiring practices and opportunities for cooperation with tech companies*. Radicalisation Awareness Network / European Commission. https://home-affairs.ec.europa.eu/system/files/2021-08/ran_extremists_use_gaming_platforms_082021_en.pdf

SEARCCT. (2023). *Building digital resilience in preventing and countering violent extremism (PCVE). Selección de artículos 2023*. <https://voxpath.eu/file/building-digital-resilience-in-preventing-and-countering-violent-extremism/>

Sugiura, L. (2021). *The incel rebellion: The rise of the manosphere and the virtual war against women*. Emerald Group Publishing.

Sunstein, C. R. (2017). *#Republic: Divided democracy in the age of social media*. Princeton University Press. <https://www.jstor.org/>

The Guardian. (2025a, 6 de noviembre). *Far-right extremists outnumber Islamists in Prevent anti-terror referrals, data shows*. The Guardian. <https://www.theguardian.com/uk-news/2025/nov/06/far-right-extremists-outnumber-islamists-prevent-anti-terror-referrals-data>

The Guardian. (2025b, 11 de noviembre). *German man with alleged neo-Nazi links arrested over darknet assassination calls*. The Guardian. <https://www.theguardian.com/world/2025/nov/11/german-man-with-alleged-neo-nazi-links-arrested-over-darknet-assassination-calls>

The Telegraph. (2026, 4 de enero). *Neo-Nazi group preparing for 'race war' in Britain*. The Telegraph. <https://www.telegraph.co.uk/news/2026/01/04/neo-nazi-group-preparing-race-war-in-britain/>

Universidad Complutense de Madrid. (s.f.). *Investigación sobre la manosfera y movimientos antifeministas online*. Proyecto Manosfera UCM. <https://www.ucm.es/manosfera/noticias/69068>

United Nations Office of Counter-Terrorism. (2022a). *Examining the Intersection Between Gaming and Violent Extremism*. United Nations. https://www.un.org/counterterrorism/sites/www.un.org.counterterrorism/files/221005_research_launch_on_gaming_ve.pdf

United Nations Office of Counter-Terrorism. (2022b). *Examining the Intersection Between Gaming and Violent Extremism – Executive Summary*. United Nations. <https://www.un.org/counterterrorism/sites/www.un.org.counterterrorism/files/video-games-exec-summary-web.pdf>

United Nations Office on Drugs and Crime (UNODC). (2023). *The use of the internet for terrorist purposes: Contemporary trends and operational challenges*. United Nations. <https://www.unodc.org/>

UNICRI. (2025). *Level Up – Gaming and violent extremism in Africa*. https://unicri.org/sites/default/files/2025-11/Level%20Up%20%E2%80%93%20Gaming%20and%20Violent%20Extremism%20in%20Africa%202025_0.pdf

UN Women. (s.f.). *¿Qué es la machoesfera y por qué debe importarnos?* [Artículo explicativo]. <https://www.unwomen.org/es/articulos/articulo-explicativo/que-es-la-machoesfera-y-por-que-debe-importarnos>

Vicente, M. (2024). *Radicalización yihadista en España: menores, espacios virtuales y la resonancia de conflictos internacionales*. Real Instituto Elcano. <https://www.realinstitutoelcano.org/analisis/radicalizacion-yihadista-en-espana-menores-espacios-virtuales-y-la-resonancia-de-conflictos-internacionales/>

Vidino, L., & Hughes, S. (2018). *A Review of Transatlantic Best Practices for Countering Radicalisation in Prisons and Terrorist Recidivism*. Europol.

von Behr, I., Reding, A., Edwards, C., & Gribbon, L. (2013). *Radicalisation in the Digital Era: The Use of the Internet in 15 Cases of Terrorism and Extremism* (Report RR-453-RE). RAND Europe. https://www.rand.org/content/dam/rand/pubs/research_reports/RR400/RR453/RAND_RR453.pdf

Wan Rosli, W. R. (2024). Violent extremism and artificial intelligence: A double-edged sword in the context of ASEAN. *Commonwealth Cyber Journal*, 2(1). <https://thecommonwealth.org/publications/commonwealth-cyber-journal-volume-2/violent-extremism-and-artificial-intelligence-double-edged-sword-context-asean>

Ware, J. (2023). *The Third Generation of Online Radicalization*. Program on Extremism, George Washington University. <https://extremism.gwu.edu/sites/g/files/zaxdzs5746/files/2023-06/third-generation-final.pdf>

Whittaker, J. (2022). *Online Radicalisation: What We Know*. Radicalisation Awareness Network / European Commission. https://home-affairs.ec.europa.eu/system/files/2023-11/RAN-online-radicalisation_en.pdf



OIET

OBSERVATORIO INTERNACIONAL
DE ESTUDIOS SOBRE TERRORISMO



COVITE

Colectivo de Víctimas
del Terrorismo