Revista Científica
del Centro Universitario
de la Guardia Civil

Revista Lógos Guardia Civil

Versión
Español

Vol. 3 Núm. 2 (2025)
junio

SUMARIO

I.- COLABORACIONES

ϕ *Cooperación entre agencias de seguridad y proceso penal: ¿Parallel construction?* · *Adriano J. Alfonso Rodríguez*

II.- TRABAJOS DE INVESTIGACIÓN

ϕ *España frente a la desinformación: Desafíos híbridos y respuestas convencionales* *Juan Francisco Adame Hernández*

ϕ *La inteligencia en el punto de mira: De la teoría clásica a la implementación en la Era Digital* · *Paula Castro Castañer*

ϕ *Hacktivismo: De la protesta social a la instrumentalización estatal* · *Josué Expósito Guisado*

ϕ *Protección internacional y soberanía: El complicado balance entre derechos individuales y seguridad nacional* · *Alejandro Gómez García*

ϕ *La guerra de Nixon contra las drogas y el auge de la vigilanciafronteriza virtual en Estados Unidos* · *J. Luigi M. Kunz Saponaro*

ϕ *Violencia sexual ejercida por desconocidos en Madrid y Barcelona: Un análisis situacional* *Francisco Pérez-Fernández/ Heriberto Janosch/Enrique López López/ Francisco López-Muñoz*

ϕ *Drogas y conducción: "Tolerancia cero". Metodología del informe salival del laboratorio Synlab y criterios de homologación de la Entidad Nacional de Acreditación* *Juan Carlos Rodríguez Bello*

ϕ *La protección de las infraestructuras críticas submarinas y el fortalecimiento de la seguridad del mar Báltico: La operación Baltic Sentry de la OTAN* · *Mónica Román González*

ϕ *El capital intelectual en la Institución de la Guardia Civil y su contribución a la economía social* · *Virginia Belén Subiris Moriel*

III.- RESEÑAS DE JURISPRUDENCIA

ϕ *Reseña de Jurisprudencia Sala 2ª Tribunal Supremo* · *Javier Ignacio Reyes López*

GOBIERNO DE ESPAÑA
MINISTERIO DEL INTERIOR
GUARDIA CIVIL

Edita:
Ministerio del Interior. Secretaría General Técnica. Madrid.

Catálogo de Publicaciones de la Administración General del Estado:
https://cpage.mpr.gob.es.

Revista Logos Guardia Civil
Revista Científica del Centro Universitario de la Guardia Civil
Fecha edición: junio 2025
NIPO (papel): 126-23-018-2
NIPO (en línea): 126-23-019-8
Depósito Legal: M-3619-2023
ISSN: 2952-3249
ISSN en línea: 2952-394X

Entidad responsable:
Centro Universitario de la Guardia Civil
Área de Investigación
Paseo de la Princesa, s/n
28300 Aranjuez (Madrid)
e-mail: investigacion@cugc.es

Diseño y maquetación:
Oficina Área de Investigación

Las opiniones emitidas en esta publicación son de exclusiva responsabilidad de sus autores.
La publicación de esta Revista y su difusión se lleva a cabo de acuerdo con las políticas de acceso abierto a la producción científica. De esta forma, y con el fin de hacer llegar el conocimiento a toda la sociedad, esta Revista publica todos los artículos y demás contenidos digitales de forma libre y gratuita bajo licencia de tipo Creative Commons Atribución-NoComercial-SinDerivadas 4.0 Internacional (CC BY-NC-ND 4.0) (https://creativecommons.org/licenses/by-nc-nd/4.0/).

DIRECTOR

Dr. Félix Blázquez González. Teniente General de la Guardia Civil. Director CUGC.

REDACTOR JEFE

Blas Guillamón Campos. Teniente Coronel de la Guardia Civil. CUGC.

SECRETARIO

Oliver Cadenas Roldán. Comandante de la Guardia Civil CUGC.

CONSEJO DE REDACCIÓN

Dr. Félix Blázquez González. Teniente General de la Guardia Civil. Dtor. CUGC.

Blas Guillamón Campos. Teniente Coronel de la Guardia Civil. CUGC.

Dr. Carlos Fernández Liesa. Catedrático de Derecho Internacional Público y Relaciones Internacionales. Delegado de la UC3M en el CUGC.

Dra. Ana Mª Garrocho Salcedo. Vicedecana Estudios Internacionales – Derecho UC3M.

Dr. Francisco López Muñoz. Catedrático de Farmacología. Vicerrector Investigación y Ciencia – UCJC.

Dra. Clara Sainz de Baranda Andujar. Directora Instituto Estudios de Género – UC3M.

Dr. Manuel Díaz Martínez. Catedrático Derecho Procesal – UNED.

Dr. Jordi Gimeno Beviá. Vicedecano Investigación e Internacionalización. Facultad Derecho – UNED.

Dr. Ricardo Cuevas Campos. Vicerrector de Política Científica – UCLM

Dra. Amaya Arnáiz Serrano. Subdirectora Instituto Alonso Martinez de Justicia y Litigacion – UC3M.

Dr. Cástor M. Díaz Barrado. Catedrático Derecho Internacional Público y Relaciones Internacionales – URJC.

Carlos Berbell Bueno. Periodista. Director Diario Confilegal.

Oliver Cadenas Roldán. Comandante de la Guardia Civil. Secretario.

COMITÉ CIENTÍFICO

Dr. Félix Blázquez González. Teniente General de la Guardia Civil. Director CUGC.

Dr. Anselmo del Moral Torres. Coronel de la Guardia Civil. Director Ejecutivo CUGC.

Dr. Eduardo Martínez Viqueira. General Jefe del Mando Personal de la Guardia Civil.

Jacobo Barja de Quiroga López. Magistrado Presidente de la Sala 5ª del Tribunal Supremo.

Julián Sánchez Melgar. Magistrado. Sala 2ª del Tribunal Supremo.

Dr. Juan Díez Nicolás. Catedrático de Sociología. Miembro de la Real Academia de Ciencias Morales y Políticas.

Dr. Juan Aparicio Barrera. Editor Revista Logos Ciencia & Tecnología. Colombia.

Dr. Pablo Morenilla Allard. Catedrático Derecho Procesal – UCLM.

Dr. Jacobo Dopico Gómez-Aller. Catedrático Derecho Penal – UC3M.

Dr. Fernando Bandrés Moya. Catedrático de Medicina Legal – UCM.

Blas Guillamón Campos. Teniente Coronel de la Guardia Civil. CUGC.

Oliver Cadenas Roldán. Comandante de la Guardia Civil. Secretario.

Página oficial Revista Logos Guardia Civil

https://revistacugc.es

Página oficial CUGC

https://www.cugc.es

Revista Científica del Centro Universitario de la Guardia Civil
Revista Lógos Guardia Civil

ÍNDICE

INTRODUCCIÓN 9

I.- COLABORACIONES

Cooperación entre agencias de seguridad y proceso penal: ¿Parallel construction? 13
Adriano J. Alfonso Rodríguez

II.- TRABAJOS DE INVESTIGACIÓN

España frente a la desinformación: Desafíos híbridos y respuestas convencionales..... 37
Juan Francisco Adame Hernández

La inteligencia en el punto de mira: De la teoría clásica a un nuevo enfoque a la implementación en la Era Digital 71
Paula Castro Castañer

Hacktivismo: De la protesta social a la instrumentalización estatal 101
Josué Expósito Guisado

Protección internacional y soberanía: El complicado balance entre derechos individuales y seguridad nacional 123
Alejandro Gómez García

La guerra de Nixon contra las drogas y el auge de la vigilancia fronteriza virtual en Estados Unidos 147
J. Luigi M. Kunz Saponaro

Violencia sexual ejercida por desconocidos en Madrid y Barcelona: Un análisis situacional..... 171
Francisco Pérez-Fernández / Heriberto Janosch / Enrique López López / Francisco López-Muñoz

Drogas y conducción: "Tolerancia cero". Metodología del informe salival del laboratorio Synlab y criterios de homologación de la Entidad Nacional de Acreditación .. 197
Juan Carlos Rodríguez Bello

La protección de las infraestructuras críticas submarinas y el fortalecimiento de la seguridad del mar Báltico: La operación Baltic Sentry de la OTAN 221
Mónica Román González

El capital intelectual en la Institución de la Guardia Civil y su contribución a la economía social 257
Virginia Belén Subiris Moriel

III.- RESEÑAS DE JURISPRUDENCIA

Reseña de Jurisprudencia Sala 2ª Tribunal Supremo..... 295
Javier Ignacio Reyes López

Revista Científica del Centro Universitario de la Guardia Civil
Revista Lógos Guardia Civil

INTRODUCCIÓN

Querido lector,

Nos complace darle la bienvenida al quinto número de nuestra revista Logos Guardia Civil, editada por el Centro Universitario de la Guardia Civil. Este nuevo ejemplar recoge una selección de trabajos que abordan, desde diferentes enfoques y disciplinas, algunos de los retos más acuciantes en el ámbito de la seguridad, tanto nacional como internacional.

Abrimos este número con la colaboración de Don Adriano J. Alfonso Rodríguez, Doctor en Derecho y Profesor de Derecho-Criminología de la UNED, quien nos ofrece una reflexión oportuna sobre la "Cooperación entre agencias de seguridad y procesos de integración regional en América Latina".

En la sección de artículos de investigación, Don Juan Francisco Adame Hernández, Director de Estrategia, Comunicación y Promoción de la Casa Árabe, nos presenta "España frente a la desinformación: Desafíos híbridos y respuestas convencionales", un estudio riguroso sobre los riesgos de la desinformación en la seguridad del Estado.

La experta de seguridad y doctoranda en Ciencias Forenses por la Universidad de Alcalá, Paula Castro Castañer nos introduce en "La inteligencia en el punto de mira: de la Teoría Clásica a la implementación en la Era Digital", un enfoque crítico sobre la percepción social de los servicios de inteligencia.

El trabajo de Josué Expósito Guisado, sargento de la Guardia Civil y doctorando en la Universidad Pablo de Olavide, titulado "Hacktivismo: de la protesta social a la instrumentalización estatal", analiza los límites entre la acción digital y la ilicitud penal.

Alejandro Gómez García, Capitán de la Guardia Civil y Máster en Dirección Operativa de la Seguridad, profundiza en la "Protección internacional y soberanía: el complicado balance entre derechos individuales y Seguridad Nacional", una cuestión de gran sensibilidad en el derecho internacional.

Don Johannes Luigi Maria Kunz Saporano, investigador doctoral en la Universidad Carlos III de Madrid, analiza en su artículo "La guerra de Nixon contra las drogas y el auge de la vigilancia fronteriza virtual en Estados Unidos" la transformación de la seguridad en EE. UU., señalando cómo las políticas impulsadas durante la 'war on drugs' dieron paso al desarrollo de sofisticados sistemas de control fronterizo apoyados en la tecnología avanzada.

El equipo formado por Francisco Pérez-Fernández, Heriberto Janosch, Enrique López López y Francisco López-Muñoz presenta la "Violencia sexual ejercida por desconocidos en Madrid y Barcelona: un análisis situacional", se trata de un estudio que aporta claves relevantes sobre la distribución geográfica y los patrones de comportamiento en agresiones sexuales urbanas.

Juan Carlos Rodríguez Bello, Cabo 1º de la Agrupación de Tráfico de la Guardia Civil, experto Universitario en Delincuencia Vial y Perito Judicial en Documentoscopia por la UNED, firma el artículo "Drogas y conducción: Tolerancia cero. Metodología del informe salival del laboratorio Synlab y criterios de homologación de la Entidad Nacional de Acreditación", en donde se abordan los estándares científicos y legales en la detección de sustancias.

Mónica Román González es doctoranda en el Programa de Ciencias Políticas y de la Administración y Relaciones Internacionales de la Universidad Complutense de Madrid, y nos ofrece un análisis estratégico en "La protección de las infraestructuras críticas submarinas y el fortalecimiento de la seguridad del mar Báltico: la operación Baltic Sentry de la OTAN", destacando la importancia de la cooperación internacional en escenarios marítimos.

Para terminar, Virginia Belén Subiris Moriel, doctoranda en la Universidad Rey Juan Carlos, Programa Ciencias Sociales y Jurídicas, cierra con "Economía Social: La contribución de la Institución de la Guardia Civil a través de su capital intelectual", un artículo que explora el valor del conocimiento compartido y el compromiso institucional con el desarrollo social.

Por otro lado, la sección de reseñas jurisprudenciales cuenta en esta ocasión con una nueva contribución de Javier Ignacio Reyes López, Magistrado Juez Decano de Alcalá de Henares, quien analiza sentencias relevantes de la Sala Segunda del Tribunal Supremo.

Desde el comité editorial agradecemos sinceramente tanto a los autores por su rigurosidad y compromiso, como a los evaluadores externos por su indispensable labor. Deseamos que esta nueva edición les resulte de interés y contribuya al conocimiento, la reflexión y la mejora continua en el campo de la seguridad.

Félix Blázquez González
Director del CUGC

Revista Científica
del Centro Universitario
de la Guardia Civil

Revista Lógos Guardia Civil

I.- COLABORACIONES

Revista Científica del Centro Universitario de la Guardia Civil
Revista Lógos Guardia Civil

Colaboración

COOPERACIÓN ENTRE AGENCIAS DE SEGURIDAD Y PROCESO PENAL: ¿PARALLEL CONSTRUCTION?

Adriano J. Alfonso Rodríguez
Doctor en Derecho
Profesor Derecho-Criminología UNED-Lugo. Juez (s)
ajalfonsorodriguez@hotmail.com
ORCID: 0009-0005-2821-4603

Recibido 14/05/2025
Aceptado 14/05/2025
Publicado 27/06/2025

Cita recomendada: Alfonso, A. J. (2025). Cooperación entre agencias de seguridad y proceso penal: ¿Parallel Construction?. *Revista Logos Guardia Civil*, 3(2), p.p. 13–34.

Licencia: Este artículo se publica bajo la licencia Creative Commons Atribución-NoComercial-SinDerivadas 4.0 Internacional (CC BY-NC-ND 4.0)
Depósito Legal: M-3619-2023
NIPO en línea: 126-23-019-8
ISSN en línea: 2952-394X

ORCID: 0009-0005-2821-4603

COOPERACION ENTRE AGENCIAS DE SEGURIDAD Y PROCESO PENAL: ¿PARALLEL CONSTRUCTION?

Sumario: 1. PREFACIO. 2. EL MODELO DE AUTORIZACION JUDICIAL PARA ACTIVIDADES DEL CNI 3. EL MODELO NORTEAMERICANO: LA FISA COURT Y UN MURO QUE SE CAE 4. LA "CONSTRUCCION PARALELA" Y LA COMUNICACIÓN DE INTELIGENCIA ENTRE AGENCIAS 5. CONCLUSIONES 6. REFERENCIAS BIBLIOGRAFICAS.

Resumen: La existencia de dos tipos de seguridad, la nacional y la pública, ha servido para apoderar a organismos diferentes sobre su prevención. Los servicios secretos han adquirido un protagonismo destacado en lo que respecta a la nacional, mientras que la pública implica la presencia de órganos policiales. Para el trabajo de vigilancia y protección es necesario en ambos casos vulnerar, autorizadamente, los derechos fundamentales. Sin embargo, no existe el mismo estándar cuando participan los servicios secretos que se ve rebajado por no estar investigando un hecho delictivo y la problemática comunicación de la información obtenida, cuando aquel aparece, a las fuerzas policiales ¿Es necesaria una estrategia de ocultación de la fuente? ¿Es precisa, en definitiva, una construcción paralela?

Abstract: The existence of two types of security, national and public, has served to empower different agencies to prevent it. Secret services have taken on a prominent role in national security, while public security requires the presence of police forces. Surveillance and protection work requires, in both cases, the authorized violation of fundamental rights. However, the same standards do not exist when secret services are involved, and they are lowered by not investigating a crime and the problematic communication of information obtained when it becomes available to police forces. Is a strategy of concealing sources necessary? Is a parallel construction ultimately necessary?

Palabras clave: Seguridad pública, Seguridad nacional, Policía, Servicio de inteligencia, Garantías procesales.

Key Words: Public security; National security; Police; Intelligence service; procedural guarantees.

ORCID: 0009-0005-2821-4603

ABREVIATURAS

Art.: Artículo.

CE: Constitución Española.

CP: Código Penal.

CESID: Centro Superior de Información de la Defensa.

CIA: Central Intelligence Agency.

CITCO: Centro de Inteligencia para el Terrorismo y Crimen Organizado.

CNI: Centro Nacional de Inteligencia.

DEA: Drug Enforcement Agency.

DIA: Defence Intelligence Agency.

EM: Exposición de Motivos.

FBI: Federal Bureau of Investigation.

FJ: Fundamento Jurídico.

LOPJ: Ley Orgánica del Poder Judicial.

LOPSC: Ley Orgánica de Protección y Seguridad Ciudadana.

LSN: Ley de Seguridad Nacional.

NSA: National Security Agency

SAN: Sentencia Audiencia Nacional.

SECED: Servicio Central de Documentación.

SED: Secretario de Estado Director.

SIAM: Servicio de Información del Alto Estado Mayor.

STC: Sentencia del Tribunal Constitucional.

STS: Sentencia del Tribunal Supremo.

TS: Tribunal Supremo

1. PREFACIO.

Desde los atentados a las Torres Gemelas en New York el 11 de septiembre de 2001-con su dolorosa réplica el 11 de marzo de 2006 en Madrid- estamos ante un mundo convulso, donde los sistemas democráticos tienen diversos frentes abiertos, frentes que comprenden desde conflictos bélicos al crimen organizado transnacional, con el telón de fondo de los persistentes riesgos terroristas, o las tareas de espionaje llevadas a cabo por países hostiles. También, de factura menos convencional, hay que estar alerta frente a los ciberataques o las campañas de desinformación, responder a los flujos migratorios irregulares, las catástrofes climáticas y pandemias globales, o la inseguridad económica. Hechos que reflejan un mundo lejano de una paz perpetua y expresivo de una "Sociedad del Riesgo" que implica confrontar una situación de intranquilidad, no provocada por amenazas sino por los individuos que las ponen de manifiesto (Beck, 2006, p. 107).

Afrontar los desafíos que se presentan, todos ellos muy variados, con raíces diferentes y soluciones complejas, nos sitúan en el ámbito de la denominada protección de la "Seguridad Nacional", concepto que se ha intentado explicar desde diversas perspectivas. No obstante, en nuestro país la regulación sobre aquella es muy reciente, apenas diez años, y busca dotar de un marco normativo a un espacio que, tradicionalmente, se situaba en la penumbra al estimar que la acción del Estado, en determinados ámbitos, debía mantenerse en un estricto secreto y ello, en claro contraste, con la idea de "Seguridad Pública" cuya presencia legislativa es muy anterior, obligada en democracia, y basada en la idea que gobernar implica una potestad de contención del poder policial (Zaffaroni, 2006, p. 165).

En todo caso, nuestro texto constitucional (en adelante CE) no ha abordado la idea de la "Seguridad Nacional", ni contempla como tal una definición, aunque sí alude al concepto de "Seguridad Pública" en diversos preceptos de nuestra lex superior al establecer la garantía de la "seguridad ciudadana" por la fuerzas de policía (art. 104.1 CE) o la titularidad estatal exclusiva de la "seguridad pública" (art. 149.1.29ª CE), sin olvidar el art. 126 CE donde habla de una "Policía Judicial" en situación de dependencia de Jueces y Fiscales en la averiguación del delito y el descubrimiento del delincuente (*Cfr.* las SSTC 175/1999, de 30 de septiembre, FJ 7º 86/2014, de 29 de mayo, FJ 4º o 55/1990, de 28 de marzo, FJ 5º). Esta situación, ayuna de reconocimiento, no ha impedido que la idea de "Seguridad Nacional" aflore como herramienta singular de protección, como una política propia, aunque sin ministerio que la gestione (Herbon Costas, 2021, p. 164). Ahora bien, lo anterior no impide observar que ambas "seguridades" operan en los mismos ámbitos, tocan aspectos semejantes y se fijan idénticos objetivos, y si bien cabe la conculcación de derechos fundamentales en ambos planos, se opera bajo diferentes criterios, más flexibles en su dimensión ética cuando se trata de cuestiones de seguridad nacional, y que dejan en el aire la existencia de un puente por el que transitar en los supuestos de colaboración entre los diferentes órganos operativos encargados de vigilar su satisfacción.

Desde una perspectiva normativa, la Ley 36/2015, de 28 de septiembre de Seguridad Nacional (en adelante LSN), señala en su art. 3 que *"*A los efectos de esta ley se entenderá por Seguridad Nacional la acción del Estado *dirigida a proteger la libertad, los derechos y bienestar de los ciudadanos, a garantizar la defensa de España y sus principios y valores constitucionale*s, así como a contribuir junto a nuestros socios y aliados a la seguridad internacional en el cumplimiento de los compromisos asumidos*"*.

Al hilo de esta definición, la idea de "Seguridad Pública" de la Exposición de Motivos (EM) de la Ley Orgánica 4/2015, de 30 de marzo, de Protección de la Seguridad Ciudadana (LOPSC) señala que "La Ley, de acuerdo con la jurisprudencia constitucional, parte de un concepto material de seguridad ciudadana entendida como actividad *dirigida a la protección de personas y bienes y al mantenimiento de la tranquilidad de los ciudadanos*, que engloba un conjunto plural y diversificado de actuaciones, distintas por su naturaleza y contenido, orientadas a una misma finalidad tuitiva del bien jurídico así definido. Dentro de este conjunto de actuaciones se sitúan las específicas de las organizaciones instrumentales destinadas a este fin, en especial, las que corresponden a las Fuerzas y Cuerpos de Seguridad, a las que el artículo 104 de la Constitución *encomienda proteger el libre ejercicio de los derechos y libertades y garantizar la seguridad ciudadana…*".

Es fácilmente perceptible, como se ha destacado, la idea común de protección de libertades y derechos que sitúan ambos conceptos en un hilo de conexión claro, que podemos observar, incluso, jurisprudencialmente. En este sentido, la STC 184/2016, de 3 de noviembre, primera resolución que ha abordado el concepto de "Seguridad Nacional" señala "*Por otra parte, siendo clara la competencia estatal, tanto en materia de defensa como en materia de seguridad pública, no tendría sentido que, en un ámbito como la seguridad nacional, tan estrechamente vinculado a ambas, hasta el punto de identificarse sus fines y objetivos y los bienes jurídicos protegidos en la forma indicada, la competencia estatal pasara a ser puramente residual. En definitiva, la seguridad nacional no es una competencia nueva,* ***sino que se integra*** *en las competencias estatales de defensa y seguridad pública*" (FJ 3º). Esta sentencia que no hace sino más que hermanar ambos conceptos, no impide que establezcamos patentes diferencias.

En primer lugar, la defensa de la seguridad nacional frente a sus amenazas, mediante la obtención de información, es materia propia de los servicios secretos, en concreto, y en nuestro país, del Centro Nacional de Inteligencia (CNI). En el caso de la seguridad pública, o ciudadana, su protección se encomienda a los servicios policiales ya sean del gobierno central, autonómico o local. En segundo lugar, los servicios secretos, en la vigilancia de aquellas actividades que puedan afectar a la seguridad nacional (espionaje, contraespionaje, labores antiterroristas...), operan bajo un criterio claro de discreción operativa extrema de manera que su trabajo queda bajo el paraguas de la información clasificada, que no es conocida por el público, y rara vez se sustancia el resultado de su trabajo ante un tribunal, situaciones éstas que no afectan al trabajo de las fuerzas de seguridad quienes desarrollan sus actividades de manera supervisada por los órganos judiciales, con resultados que son públicos y publicitados siendo la finalidad última desembocar, de ordinario, en la determinación, o no, de una responsabilidad penal a dilucidar judicialmente. En cuarto lugar, la vulneración organizada de los derechos fundamentales exige, tanto en el trabajo policial como en la tarea del CNI, una autorización judicial, sin embargo, mientras el marco procesal penal que deriva de la Ley de Enjuiciamiento Criminal (LECRIM) hace de brida a las agencias de seguridad pública, los servicios secretos operan en un marco necesariamente más amplio donde la regulación normativa es más bien limitada, a través del único artículo contenido en la Ley 2/2002, de 6 de mayo, con una supervisión judicial ceñida a la autorización de las medidas que afectan al secreto de las comunicaciones y entradas domiciliarias que afectan parcialmente al art. 18 CE siendo su finalidad la recopilación de información cuyo destino no es, en principio, un juicio. No obstante, se nos suscitan varias preguntas ¿Cómo es nuestro modelo de supervisión judicial de las actividades de inteligencia? ¿Es posible que

los servicios secretos compartan la información con las agencias policiales? ¿Sería posible su uso en el marco procesal y de investigación penal? Veamos diferentes aspectos aptos para formalizar el debate.

2. EL MODELO DE AUTORIZACION JUDICIAL PARA ACTIVIDADES DEL CNI.

La tradicional obtención de información por los servicios de espionaje siempre ha estado basada en técnicas clandestinas y con una dimensión ética necesariamente flexible en su desarrollo con un marco de garantías para los afectados bastante difuminado. Cuanto mayor es la amenaza, más complejos son los métodos de obtención de información, donde la evaluación y el análisis se convierten en herramientas de precisión para determinar la respuesta, acción o decisión. De hecho, la importancia de los servicios secretos en democracia radica en ayudar al Ejecutivo a seguir unas líneas concretas en defensa de los intereses nacionales, convirtiéndose en actores importantes para la toma de decisiones políticas (Pinto Cebrián, 2019, pp. 51 y ss.,). Nada tienen que ver con la averiguación del hecho delictivo, ni del delincuente ni su persecución procesal (Sánchez Ferro, 2020, pp. 188-189), sin olvidar que es, precisamente, la seguridad nacional la que justifica sus funciones y habilita la vulneración, ordenada eso sí, de los derechos fundamentales (Aba Catoira, 2020, p. 228).

En nuestro país, ya lo anticipé, el protagonismo lo tiene el CNI, órgano de la Administración General del Estado con una naturaleza singular (SAN 2632/2009, 27 de mayo, Sala de lo Contencioso (Ponente: Sr. Gil Ibáñez, FJ 1º), dependiente del Ejecutivo y que *"...no es ni se asimila a un organismo identificado con una administración independiente, en el sentido que tienen dicha tipología de entidades de Derecho público dotadas de la autonomía e independencia funcional que las caracteriza: es un organismo instrumental del Gobierno..."* (STS 1238/2021, de 18 de octubre, de la Sala III, (Ponente: Sr. Requero Ibáñez) FJ 7º) , que viene a reflejar, en su fisonomía, una larga evolución en la historia de nuestros servicios. Así, aquel se convierte en el sucesor del Centro Superior de Información de la Defensa (CESID) que, a su vez, fue creado por Real Decreto 1558/1977, de 4 de julio, órgano que aglutinó a los anteriores servicios de información, -Servicio Central de Información dependiente de la Presidencia del Gobierno (CESED) y Servicio de Información del Alto Estado Mayor (SIAM)-, y siempre actuando como órgano de evaluación de inteligencia y dependiente, durante los diferentes gobiernos, del Ministerio de Defensa, salvo un período de dependencia del Ministerio de Presidencia durante el gobierno de don Mariano Rajoy Brey. Su integración, inicialmente, con miembros de las Fuerzas Armadas ha acabado evolucionando con la incorporación de personal civil, de manera que ya no puede verse a este órgano como un mero recopilador de inteligencia militar ante un conflicto bélico potencial. Su trabajo va más allá, por cuanto las amenazas son cada vez más heterogéneas, con conflictos asimétricos, que se desarrollan en campos de batalla invisibles y cuya existencia e intervención resulta fundamental para confrontarlas.

Al frente del CNI, conforme el art. 9 de la Ley 11/2002, de 6 de mayo, se sitúa un Secretario de Estado **(**SED**)**, siendo "Autoridad Nacional de Inteligencia y Contrainteligencia" con el título de "Director", nombrado por Real Decreto a propuesta del Ministerio de Defensa, y con un mandato de cinco años pudiendo ser prorrogado sucesivamente o sustituido en cualquier momento por el Gobierno. Sus funciones son de "impulso" y "coordinación", que podemos resumir en "dirección" de las tareas del

ORCID: 0009-0005-2821-4603

órgano, nombramiento de los diferentes cargos directivos, competencia presupuestaria o la cooperación "*con los servicios de información de las Fuerzas y Cuerpos de Seguridad del Estado*, y los órganos de la Administración civil y militar, relevantes para los objetivos de inteligencia...". Se ve asistido por un Secretario General, con categoría de Subsecretario, que, entre otras funciones, además de sustituirlo, se encarga de "Dirigir el funcionamiento de los servicios comunes del Centro a través de las correspondientes instrucciones y órdenes de servicio" (art. 10, Ley 11/2002). Son, estos, por tanto, los principales directivos que se encargan de funciones de responsabilidad en el CNI, con la posible e hipotética existencia de la División de Inteligencia Exterior, División de Contrainteligencia, División de Inteligencia Interior, División de Economía y Tecnología junto con la Subdirección General de Administración y Servicios y Subdirección General de Personal y una Asesoría Jurídica, un Gabinete Técnico, una Jefatura de Apoyo Operativo y un Servicio de Seguridad (arts. 1 y 2 RD 2632/1985, de 27 de diciembre, si bien con posterioridad, en el RD 266/1996, de 16 de febrero, el art. 2 establecía la existencia de unidades de inteligencia y unidades de apoyo operativo y técnico junto con una unidad de seguridad encargada de tareas de protección). En todo caso, es posible que esta organización interna, a día de hoy, sea muy distinta.

De entre todas las cuestiones, hay una que subyace con importancia frente a una historia que situaba el trabajo de nuestro servicio secreto en la penumbra. Se trata de los supuestos de actividades de inteligencia en las que practicaban allanamientos y escuchas telefónicas sobre objetivos, escenario huérfano de toda regulación y enormemente problemático hasta la Ley 2/2002, de 6 de mayo, que en un único precepto, con incidencia a través de su derecho transitorio en la Ley Orgánica del Poder Judicial 6/1985, de 1 de julio, (LOPJ), en los arts. 125, 127, 135, junto con el nuevo art. 342 bis en el mismo texto, decide que sea un Juez del Tribunal Supremo (Sala Segunda de lo Penal o Tercera de lo Contencioso-Administrativo) el encargado de la autorización al CNI de actos que afecten a la inviolabilidad domiciliaria (art. 18.2 CE) y la interceptación de comunicaciones (art. 18.3 CE). Configurando un sistema insólito (Lanz Muniain, 2023, p.27), sin parangón en los países de nuestro entorno, excepción hecha, con relativos matices, de los Estados Unidos como veremos, la atribución de la competencia a una magistratura unipersonal, y temporal por espacio de cinco años, no está exenta de críticas por apartarse del sentido constitucional de Juez ordinario predeterminado por la Ley (De la Oliva Santos, 2006, p. 154). Es evidente que no se ha creado, propiamente, una corte de espionaje.

La justificación que se hace para la modificación resulta de la EM de la Ley 2/2002 que señala "Para las actividades que puedan afectar a la *inviolabilidad del domicilio y al secreto de las comunicaciones*, la Constitución española exige en su artículo 18 autorización judicial, y el art. 8 del Convenio Europeo para Protección de los Derechos Humanos y de las Libertades Fundamentales exige que esta injerencia esté prevista en la Ley y constituya una medida que, en una sociedad democrática, *sea necesaria para la seguridad nacional, la seguridad pública*, el bienestar económico del país, la defensa del orden y *la prevención del delito*, la protección de la salud o de la moral, o la *protección de los derechos y las libertades de los demás*". Como se puede observar alude a las dos seguridades y a aspectos que las nutren como elemento justificante de la vulneración del art. 18 CE y con el trasfondo de la protección de los derechos y libertades, elemento nuclear de ambas.

El modelo de autorización es sumamente peculiar, regulado en el artículo único de la Ley 2/2002, de 6 de mayo, y en síntesis se inicia por el SED quien formula al Magistrado del TS (Sala II o III), elegido por el Consejo General del Poder Judicial (CGPJ) por un período de cinco años-coincidente con el mandato del SED- para tal función, una petición de conculcación de derechos fundamentales que debe estar debidamente motivada y contener necesariamente los siguientes extremos: "*a) Especificación de las medidas que se solicitan. b) Hechos en que se apoya la solicitud, fines que la motivan y razones que aconsejan la adopción de las medidas solicitadas. c) Identificación de la persona o personas afectadas por las medidas, si fueren conocidas, y designación del lugar donde hayan de practicarse. d) Duración de las medidas solicitadas, que no podrá exceder de veinticuatro horas en el caso de afección a la inviolabilidad del domicilio y tres meses para la intervención o interceptación de las comunicaciones postales, telegráficas, telefónicas o de cualquier otra índole, ambos plazos prorrogables por sucesivos períodos iguales en caso de necesidad*". Recibida la petición impetrada por el SED, el Juez del TS tiene 72 horas (o 24 horas en función de la urgencia de la medida) salvaguardando sus actuaciones, que serán secretas. La inicial resolución judicial, posiblemente un auto, y las posteriores que las prorrogan, ni son recurribles, ni tampoco revisables, y ello porque los únicos actores de dicho procedimiento son el Magistrado del TS y el SED, quien, por otro lado, "ordenará la inmediata destrucción del material relativo a todas aquellas informaciones que, obtenidas mediante la autorización prevista en este artículo, no guarden relación con el objeto o fines de la misma".

A la vista está que no existen principios que inspiran la petición, criterios de concesión o denegación, uso o destino del material obtenido, control judicial de la ejecución de las medidas o del resultado obtenido, excepción hecha de la prórroga, situación de los afectados por la medida de inmisión o recursos a interponer frente a la resolución dictada. En este sentido, la justificación pasa, apriorísticamente, porque el material obtenido ni es susceptible de generar acervo probatorio ni va a ser utilizado en el proceso penal (González Cussac, 2015, p.88). No obstante, no podemos descartar, como primer elemento de matiz, la trascendencia procesal del trabajo de inteligencia pues destaca el uso, en la jurisdicción contenciosa, de los informes del CNI para denegar la nacionalidad de solicitantes extranjeros por motivos de "seguridad nacional" (SSTS 233/2022, 23 de febrero, de la Sala III, Ponente: Sr. Menéndez Pérez, FJ 4º; 395/2022, 29 de marzo, de la Sala III, Ponente: Sr. Román García FJ 6º; 367/2021, de 17 de marzo, de la Sala III, Ponente: Sr. Herrero Pina FJ 2º,; 4376/2015, de 26 de octubre, de la Sala III, Ponente: Sr. Del Riego Valledor, FJ 4º; STS 2105/2014, de 26 de mayo, de la Sala III, Ponente: Sr. Del Riego Valledor, FJ 5º). No obstante, sobre su empleo en procesos penales volveré más adelante para clarificar la cuestión. En todo caso, se ha buscado conjugar aspectos relativamente antitéticos como supervisar algo que, por su propia naturaleza podría no serlo, mediante la apertura de una vía judicial que, por otro lado, no encorseta operativamente a los agentes al mantenerlos al margen de las exigencias derivadas de la existencia de un proceso penal abierto (Alfonso Rodríguez, 2024, p. 132).

El punto de inicio de la solicitud pivota en torno al art. 4 b) de la Ley 11/2002, de 6 de mayo, que establece, entre otras, como función principal de nuestro servicio de espionaje el de " *Prevenir, detectar y posibilitar la neutralización de aquellas actividades de servicios extranjeros, grupos o personas que pongan en riesgo, amenacen o atenten contra el ordenamiento constitucional, los derechos y libertades de los ciudadanos españoles, la soberanía, integridad y seguridad del Estado, la estabilidad de sus*

instituciones, los intereses económicos nacionales y el bienestar de la población". En este sentido, aquí se refleja el elemento justificativo de la solicitud de autorización judicial del artículo único, convirtiendo al Juez del TS autorizante en intérprete de conceptos no jurídicos como "soberanía" o "integridad", "intereses económicos nacionales" o el "bienestar de la población" que son las finalidades últimas del desarrollo de las tareas de espionaje y que juntamente con el respeto a los derechos, libertades o estabilidad institucional implica convertirlo en el guardián de la "seguridad nacional" que apodera al servicio para poder desarrollar sus funciones.

La cuestión que suscita la habilitación judicial al CNI para interceptar un teléfono o entrar en un domicilio es que supone una suerte de salvaguarda pero se distancia de una función de garantía de los derechos fundamentales (Pascual Sarria, 2007, p. 197) que, por otro lado, el Poder Judicial tiene atribuido en virtud del art. 117.4 CE, y convierte el procedimiento en *una suerte de expediente secreto de solicitud de medidas limitativas de derechos fundamentales concretos, en el marco de operaciones de inteligencia para la protección de la seguridad nacional, a un Juez del TS, sometido a un mandato temporal y expresamente nombrado para tal fin* (Alfonso Rodríguez, 2023, p.89).

3. EL MODELO NORTEAMERICANO: LA FISA COURT Y UN MURO QUE SE CAE.

No está claro si los Estados Unidos han sido el modelo seguido para la configuración y fisonomía de nuestro sistema de control de actividades inteligencia. Ahora bien, resulta claro que no podemos aceptar la inspiración total pues el sistema procesal es distante entre ambos países, existiendo el esquema adversarial de Norteamérica en el que las partes (acusador y acusado) son las verdaderas "dueñas" del proceso penal estadounidense, y donde el principio del "Due Process of Law", el derecho al proceso debido con todas las garantías, se nos muestra como el "motor" de la organización procesal (Gómez Colomer, 2006, pp. 50-57), en contraste con un modelo de Juez Instructor que resulta bendecido por una LECRIM de 1882, imposible, bajo cualquier presupuesto, en Estados Unidos. No obstante, hay que señalar que el modelo procesal de la FISA Court no responde a este sistema de adversarios.

El modelo de inteligencia norteamericano se asienta sobre una pluralidad de agencias (CIA, NSA, DIA, FBI en su rama de inteligencia, Fuerzas Armadas y Departamentos del Gobierno con sus propios servicios) que ahora son coordinadas por un Director/a Nacional de Inteligencia, con arreglo a la Ley de Reforma de Inteligencia y Prevención del Terrorismo de 2004 (IRPA) en cuanto comisionado del Ejecutivo para una adecuada coordinación de todas las organizaciones, conviviendo con un intenso control por parte del legislativo a través de las comisiones parlamentarias de supervisión. Sentada esta circunstancia, hay que partir de una fase de abusos sistemáticos por parte del FBI o la CIA puestos de manifiestos por el Comité *Church* del Senado (Arrieta, 2025, p. 122), motivó que se promulgase en 1978 la *Foreign Intelligence Surveillance Act* (FISA) o Ley de Vigilancia de Inteligencia Extranjera, siendo parte de ella la creación de un Tribunal Federal destinado a controlar la vigilancia electrónica de los agentes extranjeros en Estados Unidos, integrada ahora por once Jueces Federales con identidades públicas pero con un trabajo que se desarrolla en secreto, y que son designados por el Presidente (*Chief Justice*) de la Corte Suprema Federal de los Estados Unidos. Son estos Magistrados los que se encargan de verificar las peticiones del Ejecutivo quien debe acreditar como "causa probable"-sospecha sensata que motiva la solicitud- que el objetivo de la escucha o

vigilancia de los dispositivos electrónicos es un poder extranjero o agente de un poder extranjero destinatario de la operación de recopilación de inteligencia, por tanto, su uso no estaba, apriorísticamente, destinado a interceptar las comunicaciones de ciudadanos norteamericanos. Al no tener que acreditarse indiciariamente la comisión de hecho delictivo alguno para conseguir el mandato del Tribunal FISA, el standard de autorización es menos riguroso que el habitual que se solicita policialmente para conculcar los derechos de la cuarta enmienda-privacidad- (Ruger, 2007, p. 243).

La solicitud se sustancia ante un Juez del Tribunal FISA en la que el Gobierno comparece con su representación como única parte procesal interviniente donde, además, de acreditar la causa probable debe señalarse la identidad de los implicados y de los funcionarios actuantes, duración de las medidas de vigilancia electrónica, certificados de las autoridades de inteligencia y detalle de solicitudes anteriores, entre otros elementos. El hecho que sea el Ejecutivo quien actúa como único participe permite distanciar su procedimiento del sistema adversarial propio del sistema norteamericano (Sobel, 2023, p. 15), estimando que efectivamente una de las razones, entre otras expuestas en su momento por el Ministro de Justicia (*Attorney General*) Griffin Bell durante la elaboración de la Ley, que podría motivar la falta de otros actuantes, vendría dada por la reticencia del propio Gobierno a desclasificar información por temor a filtraciones (Chin, 2021, p.665).

A la vista de los datos suministrados, el Juez FISA concederá, o denegará detalladamente, la orden (*warrant*) de vigilancia electrónica interesada por el Gobierno con identificación de sujetos, medios, tipo de información a obtener y duración de dicha orden siendo su denegación revisable ante la *FISA Court Review* integrada por tres jueces del mismo órgano, siendo posible interponer apelación ante la Corte Suprema (*U.S Supreme Court*) si la revisión no obtiene el éxito el pretendido.

Sin embargo, si bien hasta el año 2001 el mandato FISA servía para acopiar inteligencia, los ataques terroristas del 11-S en Estados Unidos, con la Ley Patriótica (*Patriot Act*) de 2001, en virtud de la sección 203, mutó la arquitectura de la ley y con ello rompió la separación (*wall*) entre recopilación de inteligencia extranjera e investigaciones criminales (Donohue, 2021, p. 204), permitiendo el uso de información-compartición por las agencias policiales (FBI o la DEA), obtenida bajo el fin de recopilación de inteligencia extranjera a la luz de FISA, y en investigaciones criminales, mezclando de esta manera un idéntico método con finalidades distintas lo que motiva varias reflexiones.

En primer lugar, en virtud de los estándares de petición por cuanto la acreditación de la causa probable es distinta, pues en una investigación penal había que evidenciar, a través de aquel concepto, la posible comisión de un hecho delictivo, esto no es algo que acontece en la petición de orden bajo la regulación FISA. En segundo lugar, con el objetivo común de la prevención de un ataque terrorista se incrementaba la cooperación y transmisión de inteligencia entre las agencias de espionaje y las fuerzas de seguridad cuyos cometidos son diferentes, y así los límites entre Comunidad de Inteligencia y agencia policial se difuminaban y mezclaban (Stein, Mondale, Fisher, 2016, p. 2266). En tercer lugar, la posibilidad de construir un caso criminal, con información obtenida bajo los criterios de la FISA, se convertía en una posibilidad evidente (pensemos en un caso federal de terrorismo o narco- terrorismo en el que las fuerzas policiales han recibido información de las agencias de inteligencia fruto de los resultados obtenidos en virtud de

una orden FISA) de manera que se planteaba un claro debate respecto de las garantías procesales de los afectados y su derecho de defensa ante la compartición de materiales de inteligencia entre agencias (Reid, 2015, p. 429).

4. LA "CONSTRUCCION PARALELA" Y LA COMUNICACIÓN DE INTELIGENCIA ENTRE AGENCIAS.

Fruto de lo anteriormente observado respecto de la caída del muro, se evidencia que la "Seguridad Nacional", concepto demasiado ambiguo, embebía a la "Seguridad Pública", teniendo presente que los requisitos procesales de conculcación de derechos fundamentales, singularmente, la privacidad de las comunicaciones se veían rebajados ante la pretensión de recopilación de inteligencia, inteligencia que luego, fruto de un cambio de realidades, que motivaban una mutación de principios, se usaba con fines distintos de manera que se bordeaban las aduanas procesales y los derechos fundamentales en ejercicios de intercambiabilidad, ya fuera para la toma de decisiones políticas, ya fuera para configurar una base destinada un caso penal. Es, en este escenario, donde cobra sentido el concepto de *"construcción paralela"*, que se iniciaba por la recepción de información de inteligencia con estándares de obtención relajados y cuyo origen no se puede revelar y que, como antes apunté, bien pudiera poner en riesgo las garantías procesales al suponer un atajo operativo que pudiera sortear las objeciones legales y que obliga a inventarse un cauce-paralelo- que desvíe la atención de la fuente originaria (p. e. un confidente artificialmente creado que oculta la información de inteligencia obtenida de un mandato distinto como pudiera ser un warrant del Tribunal FISA).

Si antes analizamos el modelo de obtención de información por el CNI, órgano principal de nuestra Comunidad de Inteligencia, la situación ante la que se encuentra una agencia policial, ya sea estatal como la Policía Nacional, Guardia Civil o Servicio de Vigilancia Aduanera o los supuestos de Policías Autonómicas expresivas de un modelo integral (STC 184/2016, de 3 noviembre, FJ 4º) como Cataluña, Navarra y el País Vasco, teniendo cada una de ellas unidades de información y que configuran una suerte de **"**Comunidad Policial de Inteligencia" donde el Centro de Inteligencia para el Terrorismo y Crimen Organizado (CITCO) interviene como órgano de análisis y coordinación entre cuerpos. No obstante, es preciso indicar que, a la hora de recopilar inteligencia, los cuerpos policiales se ven sometidos a servidumbres procesales, en el marco de la satisfacción de la seguridad pública, radicalmente diferentes respecto de los servicios de inteligencia, y donde la autoridad judicial actúa como garante de los derechos fundamentales. En este sentido, el marco de actuación previsto en la LECRIM condiciona el paso de los investigadores sujetando su actividad a un conjunto de principios y exigencias que se establecen un estándar de garantías procesales propias del Estado de Derecho.

Una investigación penal puede incidir en diversos derechos fundamentales como la libertad personal (art. 17 CE), la intimidad (art.18.1 CE), la inviolabilidad domiciliaria (art.18.2 CE), el secreto de las comunicaciones (art. 18.3 CE) y también la libertad de circulación o movimientos (art. 19 CE) siendo la autoridad judicial que determina bajo los presupuestos de la Ley la posible adopción de cualquier medida que afecte a los anteriores, por tanto, si bien debe existir una habilitación legal que permita su adopción, esto, sin embargo, no es suficiente. Es necesario que la medida conculcadora este motivada de manera suficiente de tal modo que exprese la argumentación fáctica y

jurídica que determina su adopción con arreglo a los principios de especialidad, idoneidad, excepcionalidad, necesidad y proporcionalidad. Es decir, se tiene que estar investigando un hecho delictivo (especialidad) que en todo caso debe ser lo suficientemente grave para motivar la adopción de dicha medida, que sirva al objetivo de la investigación (idoneidad; SSTC 85/1994, 14 de marzo, FJ 3°; 181/1995, 11 de diciembre, FJ 5°; 49/1996, 26 de marzo, FJ 3°; 54/1996, 26 de marzo, FJ 7° y 8°; 123/1997, 1 de julio, FJ 4°) pues los resultados no se pueden conseguir por medio de otras medidas menos gravosas respecto a los derechos fundamentales del investigado, resultando imprescindibles desde la perspectiva del caso concreto (excepcionalidad y necesidad) y finalmente sólo hechos graves, trascendentes socialmente con indicios poderosos, justifican el sacrificio de derechos fundamentales clave so riesgo de ver una situación de impunidad delictiva (proporcionalidad, STC 49/1999, 5 de abril, FJ 7°).

A la vista está que la petición limitativa de derechos fundamentales que inste para investigar la unidad policial se ve sometida a las anteriores exigencias justificativas, de manera que, ante un hecho delictivo que está siendo objeto de investigación en curso, se encuentra con un "muro" que precisa ser saltado mediante la habilitación judicial para poder continuar con la indagación. No cabe, bajo ningún concepto, la petición policial con fines prospectivos (STS 822/2022, 18 de octubre de la Sala II (Ponente: Sr. Palomo del Arco), FJ 1º.3. a)) es decir, sin un delito previo indiciariamente justificado no cabe, si quiera pensar, en llevar a cabo una solicitud destinada a obtener una resolución judicial que conculque un derecho fundamental. Por tanto, es evidente que las fuerzas policiales están para investigar bajo parámetros precisos y limitaciones claras y si bien la clandestinidad de la indagación es precisa, su destino final es aflorar en un juicio público con pleno respeto al derecho de defensa y con el objetivo claro de satisfacer las exigencias de la "seguridad pública" (STC 175/1999 de 30 de septiembre, FJ 7º o la STC 86/2014, de 29 de mayo FJ 4º), algo que contrasta con la tarea de los servicios secretos donde, en aras de proteger la "seguridad nacional", se recopila información de personas físicas o jurídicas, nacionales o extranjeras, información que pasa a clasificarse y que, desde luego, no está destinada a ventilarse públicamente ante un órgano de enjuiciamiento para deducir una responsabilidad penal y sin que ideas como "contradicción", "defensa", "sospechoso" o "procesado" tengan sustantividad propia dado que su trabajo nada tiene que ver con la investigación criminal.

Sin embargo, pese a lo anteriormente expuesto, los campos de actuación de las fuerzas policiales y de los servicios secretos son comunes. Crimen organizado, terrorismo, inmigración ilegal...son una amenaza simultánea a la "seguridad pública" y a la "seguridad nacional" de tal manera que:

El crimen organizado es una amenaza a la seguridad que se caracteriza por su finalidad esencialmente económica, su efecto horadador sobre la instituciones políticas y sociales, su carácter transnacional y su opacidad. Los grupos delictivos y las organizaciones criminales camuflan sus operaciones ilegales con negocios lícitos y se apoyan cada vez más en tecnologías digitales, como las cripto-monedas y la Internet oscura. Además de su dimensión económica, el crimen organizado tiene un relevante potencial desestabilizador. Sus estructuras se adaptan al entorno geoestratégico y repercuten en la gobernanza, la paz social y el normal funcionamiento de las instituciones. En cuanto a la delincuencia grave, actividades como la explotación de menores o la trata con fines de explotación sexual se dirigen hacia los colectivos vulnerables y violan gravemente los derechos humanos. El contrabando, el cibercrimen, el tráfico de drogas,

de armas y de especies silvestres y la corrupción son amenazas tangibles para la Seguridad Nacional. La convergencia entre grupos terroristas y redes de crimen organizado va en aumento. Los modelos de organización cada vez más descentralizada de estos actores delictivos favorecen su cooperación y facilitan la financiación terrorista (Estrategia de Seguridad Nacional (2021), pp. 64-65).

Ni que decir tiene que, en atención a lo anteriormente señalado, es necesaria una actividad colaborativa de nuestro servicio secreto y de las fuerzas policiales en una actividad que pudiera ser materialmente coincidente en cuanto a hechos y sujetos, de ahí su naturaleza claramente concentrica cuando se trata, entre otras cuestiones, de terrorismo, crimen organizado o ambos. Llegados a este punto, se suscita una duda clara, ¿Qué ocurre cuando al CNI fruto de sus escuchas tiene conocimiento de un hecho delictivo susceptible de ser investigado por su inminencia?

Es evidente que no hay un sistema de vasos comunicantes regulado legalmente que oficialice la transmisión de información ante el conocimiento por el CNI de la comisión de hechos delictivos (Sánchez Barrilao, 2011, p. 61), pues apenas hay referencias en la Ley 11/2002, de 6 de mayo, acerca de la cooperación con las Fuerzas de Seguridad salvo aspectos puntuales como el art. 9.2 d) que atribuye al SED el mantenimiento y desarrollo de "la colaboración con los servicios de información de las Fuerzas y Cuerpos de Seguridad del Estado, y los órganos de la Administración civil y militar, relevantes para los objetivos de inteligencia". Es aquí donde entre en juego lo que antes señalamos como *"construcción paralela"* en cuanto expresión de la configuración de un caso penal por una fuerza policial ocultando el origen de la fuente que lo impulsa (Reid, 2015, p. 427) y que necesariamente podría estar conectado con una información obtenida por una agencia de inteligencia teniendo que construir elementos indiciarios paralelos destinados ser el manto que esconda la génesis de la información originaria, lo que nos obliga a ver cómo deberíamos tratar el material de inteligencia como iniciador o impulsor de una investigación policial penal.

En principio, hay que partir de lo señalado por la STS 746/2022, de 21 de julio de la Sala II, (Ponente: Sra. Polo García) que señala:

"(...) Como hemos dicho en la sentencia que es citada por la Sala -312/2021, de 13 de abril- no existe un derecho a que el encausado pueda desvelar el contenido y alcance de las colaboraciones policiales internacionales. *Los investigados sometidos a proceso penal carecen de un derecho que les ampare a desvelar los puntos de apostamiento policial, o la identidad de los confidentes, o la información recabada mediante técnicas de criminalística que perderían su eficacia si se divulgaran masivamente. No existe un derecho a conocer los instrumentos y materiales concretos de los que se dispuso la policía para la investigación y que podrían quedar desprovistos de eficacia para intervenciones futuras*. Tampoco hay un derecho a conocer las indagaciones de otros delitos que puedan atribuirse a los mismos sospechosos pero que estén todavía en proceso de confirmación policial, menos aún si consideramos que, en su caso, deberán ser objeto de un procedimiento de persecución penal independiente (art. 17.1 LECRIM). Como no resulta tampoco asumible que se conozcan aquellas investigaciones que ni siquiera afectan a los sometidos a proceso y que pueden arruinar otras actuaciones policiales de obligada persecución de la criminalidad." (FJ 3.3).

El origen de la anterior resolución se debía a la negativa del órgano judicial que se encargó del enjuiciamiento de aceptar la testifical de agentes de la DEA americana que facilitaron información a la Policía Nacional que llevó a cabo una investigación en materia de drogas que culminó con una condena. Repárese que la resolución anterior no era novedosa, nuestro Alto Tribunal ya había dejado claro con bastante anterioridad que "...cuando servicios de información extranjeros proporcionan datos a las fuerzas y cuerpos de seguridad españoles, *la exigencia de que la fuente de conocimiento precise también sus propias fuentes de conocimiento, no se integra en el contenido del derecho a un proceso con todas las garantías*..." (STS 445/2014, de 29 de mayo, de la Sala II, Ponente: Sra. Ferrer García FJ 2º ; STS 884/2012, de 12 de noviembre, de la Sala II, Ponente: Sr. Marchena Gómez FJ 8). Por tanto, obtenemos una primera solución parcial: los servicios de inteligencias extranjeros pueden facilitar a nuestras fuerzas policiales sus fuentes sin ningún problema para comenzar a investigar. Su origen, en suma, no es relevante y por tanto la DEA (o el FBI, o cualquier otra fuerza policial extranjera) podría recibir información de una agencia de inteligencia propia (CIA, NSA…o de su servicio de inteligencia) y transmitirla a agencias policiales para iniciar un caso penal en nuestro país, sin entrar en el debate de la relajación en los estándares legales de obtención, por cuanto no existe un derecho a debatir sobre las fuentes de obtención, dado que no es exigible su conocimiento para configurar el proceso debido.

La cuestión de la transmisión a las fuerzas de seguridad por parte del CNI de informaciones que ha podido obtener fruto de sus escuchas-o de las entradas domiciliarias- requiere otras precisiones y de hecho es un asunto abordado jurisprudencialmente negando que sus funciones tengan que ver con la investigación penal (SSTS 1140/2010, de 29 de diciembre, de la Sala II (Ponente: Sr. Berdugo Gómez de la Torre); 1094/2010, de 10 de diciembre, de la Sala II (Ponente: Sr. Marchena Gómez)). Y en este punto, se vuelve a insistir, la diferente metodología procedimental-procesal que requiere una interceptación telefónica, por ejemplo, dependiendo si lo solicita el CNI de si lo solicita una agencia policial es que sólo tienen en común la necesidad de la autorización judicial misma, nada más.

Argumentos a favor que una información obtenida por el CNI vulnerando un derecho fundamental, y bajo sus presupuestos procedimentales-no procesales- propios, con autorización judicial pueda servir como fuente para iniciar un caso penal con la posible comunicación a las fuerzas policiales no faltan.

En primer lugar, se impone *un principio de unidad de acción entre agencias policiales y de inteligencia* y que resulta impuesto por las Estrategias de Seguridad Nacional que se vayan dictando en cuanto marco de actuación (art. 4.3 LSN). Así:

En los ámbitos tradicionales de la seguridad, la adaptación a la naturaleza cambiante de las amenazas – conflictos armados, terrorismo, criminalidad organizada, proliferación, flujos migratorios irregulares, actividades de los Servicios de Inteligencia – es un rasgo constante de *la acción de los diversos agentes de la Seguridad Nacional*. A medida que aumenta la transnacionalidad de estos fenómenos, *se intensifica la exigencia de concertación* a todos los niveles. La estrecha vinculación que con frecuencia existe entre varias de estas amenazas obliga a abordarlas desde marcos estratégicos y operativos amplios, *bajo la premisa del principio de unidad de acción*. Del presente Informe se desprende que este enfoque tiene ya plena vigencia en la respuesta de España a los retos clásicos de la seguridad (Estrategia de Seguridad Nacional, 2013, p. 145).

ORCID: 0009-0005-2821-4603

Difícilmente, so riesgo de poner en peligro a la comunidad, no podemos admitir un trabajo configurado en compartimentos estancos y así la LSN impone esa "unidad de acción" (art. 4.2) recordando el art. 9. 2 que "Los *Servicios de Inteligencia e Información del Estado*, de acuerdo con el ámbito de sus competencias, apoyarán permanentemente al Sistema de Seguridad Nacional, proporcionando elementos de juicio, información, análisis, estudios y propuestas necesarios para prevenir y detectar los riesgos y amenazas *y contribuir a su neutralización*". Por tanto, la exigencia de un sentido convergente se concreta necesariamente en la cooperación entre agencias ("Servicios") para cumplir con las exigencias destinadas a conjurar los riesgos ("contribuir a su neutralización"). En suma, la comunicación de información es clave como elemento coadyuvante para neutralizar los riesgos que surjan.

En segundo lugar, una justificación de la comunicación podría venir dada por *la obligación de denuncia de los hechos delictivos o de su comisión inminente* de todo aquel que lo presenciare con arreglo al art. 262 LECRIM (De la Oliva Santos 2006, p. 164) empezando por el propio Magistrado del TS que autorizara la intervención de comunicaciones o la entrada en el domicilio del CNI (López Alafranca, 2014, p. 135) y ello en virtud igualmente de la exigencia de responsabilidad penal (407 y 408 CP) cuando hablemos de funcionarios policiales que pudieran prestar servicios en el CNI. El conocimiento por el Juez del desarrollo de la medida autorizada necesariamente deberá derivarse de la necesidad de prórroga de las medidas limitativas de derechos fundamentales que puede interesar el CNI, por cuanto no existe la posibilidad del desconocimiento de los hechos por el órgano autorizante salvo que se admitiese una autorización "ciega" como un "cheque en blanco" y sin control de manera sucesiva, lo que no es posible por cuanto la norma prevé dicha prórroga "en caso de necesidad" (art. único 2 d) Ley 2/2002) , necesidad que debería ser justificada, con los hechos resultantes de la medida inicialmente acordada, para continuar con las medidas limitativas.

No puede aceptarse la tesis, sin perjuicio de su solvencia, que la falta de consideración de autoridad de los agentes del CNI (art. 5.4 Ley 11/2002) enerva la obligación de denunciar delitos (Lanz Muniain, 2023, p. 34), sin embargo la obligación que el art. 262 LECRIM impone a aquellos que "por razón de sus cargos, profesiones u oficios" tengan conocimiento del hecho delictivo determina que es indiferente si se es, o no, autoridad o su agente por cuanto conoce por su profesión el hecho y debe denunciarlo. Pero es que tal comunicación ha venido a ser avalada por el propio TS al señalar que "Por tanto, la función legal de este Servicio no es la investigación de delitos concretos, sin perjuicio de que si en el curso de sus labores *averiguan* o tienen indicios de acciones delictivas *lo pongan en conocimiento de los órganos policiales y judiciales competentes*, pero -se insiste- su actividad no va encaminada directamente al descubrimiento de delitos, ni tiene como condicionante la previa comisión de alguno" (STS 1140/2010, de 29 de diciembre, de la Sala II (Ponente: Sr. Berdugo Gómez de la Torre) FJ 9º) .

En tercer lugar, *una hipotética clasificación secreta tampoco puede amparar la impunidad de hechos de naturaleza delictiva* (López Alafranca, 2014, p. 136), que, por otro lado, deben ser necesariamente impedidos. Asimismo, aun cuando se tratase de información clasificada ("organización y estructura interna, medios y procedimientos, personal, instalaciones, bases y centros de datos, fuentes de información y las informaciones o datos que puedan conducir al conocimiento de las anteriores materias.." ex art. 5.1 Ley 11/2002) , nada obstaculiza un procedimiento de desclasificación de la información a nivel procesal pero esto es una cuestión ajena a la comunicación misma

que, precisamente, tiene como límite aquella información transmitida en la que no se divulgue material que deba ser desclasificado (Pascual Sarria, 2007 p. 214).

En cuarto lugar, precisamente la obtención por el CNI de información si implica vulnerar la privacidad de las comunicaciones o la entrada en domicilio *está avalada por una resolución judicial necesariamente motivada por su efecto lesivo* (SSTC 126/1995, de 25 de julio, FJ 2; 139/1999, de 22 de julio, FJ 2; en idéntico sentido, SSTC 290/1994, de 27 de octubre, FJ 31; 50/1995, de 23 de febrero, FJ 5; 41/1998, de 24 de febrero, FJ 34; 171/1999, de 27 de septiembre, FJ 10; 8/2000, de 17 de enero, FJ 4), por tanto no se han acordado tales medidas al margen de un esquema procedimental o por un capricho acorde con sus necesidades operativas, de manera que no hay ilicitud propiamente en su obtención y por tanto, tampoco en su comunicación para el inicio de una investigación penal, investigación que no nace contaminada.

Con arreglo a esta cuestión, hay que diferenciar el aspecto probatorio de la cuestión propia de la comunicación para el inicio de causa penal. Son temas diferentes. El material obtenido por el CNI no está destinado a ser prueba en el proceso penal, y ello porque es la investigación policial misma la que está destinada a cumplir con dicha función, recordando que sólo existe "prueba ilícita" (art. 11 LOPJ) "cuando los medios empleados para obtenerlos resultan constitucionalmente ilegítimos" (STC 49/1999, de 5 de abril, FJ 12). En este sentido, la STS 1094/2010, de 10 de diciembre, en su FJ 2 A nos recuerda que "... Pero lo que está fuera de dudas *es que la existencia de un ulterior proceso penal en el que la notitia criminis no sea ajena al expediente de seguridad tramitado por el CNI, no implica la transmutación de la funcionalidad de ese expediente,* que dejaría de ser lo que es, distanciándose de sus principios reguladores, para convertirse en un acto procesal sine qua non del verdadero proceso y, por tanto, sometido a las reglas generales que disciplinan el principio de publicidad".

Y es precisamente, la decisión judicial autorizante la que impide hablar de una suerte de "cornisa" alegal por la que, arriesgadamente, transitarían nuestro servicio de inteligencia. Sin embargo, si bien hemos dicho que el material de inteligencia no va destinado al proceso penal como elemento probatorio no hay que olvidar que "Y respecto a la incorporación al proceso de las pruebas obtenidas por los Servicios de Inteligencia y que se refieran a material desclasificado, puede ser valorado desde dos prismas diferentes. O bien actúa en el proceso penal como documental, cuando se trata de una prueba de estas características, o bien sirve para conducir la investigación criminal mediante la declaración testifical de los autores del mismo" (STS 1140/2010, de 29 de diciembre, de la Sala II (Ponente: Sr. Berdugo Gómez de la Torre) FJ 9º).

Sin embargo, no faltan objeciones al sistema, empezando por las complejidades que podría implicar la presencia de los servicios secretos en el proceso penal (Hassemer, 2000, p. 114), de tal manera que podría existir una confusión, casi una mezcla, que convirtiera en indistinguibles las funciones policiales y de recopilación de inteligencia (Orgis, 2011, p. 162). No sería bueno para las fuerzas policiales, no sería bueno para los servicios secretos y ello en virtud de los diferentes parámetros de actuación. Por otro lado, la obtención de una escucha o la entrada domiciliaria por nuestros servicios secretos está sujeta a un estándar distinto donde es preciso justificar extremos propios de peligro para la seguridad nacional que puede no tener nada que ver con la comisión de un hecho delictivo. En suma, una cosa es que en el curso de una operación de inteligencia se descubriera un hecho delictivo grave, o cuya comisión fuera inminente, algo que

necesariamente debe ser comunicado o denunciado a las fuerzas policiales y otra distinta es que el procedimiento de solicitud y obtención de escuchas o entrada domiciliaria por los servicios secretos sirviera, a modo de atajo procedimental, para la búsqueda del delito mismo lo que avocaría a la irrelevancia del sistema de garantías procesales constitucionales en lo referido a la limitación y conculcación de derechos fundamentales.

Finalmente, antes apuntamos que no toda la información puede ser conocida lo que podría llevar, ya en el marco de un proceso penal, a poner a prueba el derecho de defensa (art. 24.2 CE) pues el acceso al expediente en el caso del CNI está sometido a restricciones y a una situación de clasificación que contrasta con la puesta a disposición de las partes implicadas de todos los elementos integrantes de la instrucción penal. Es decir, la presencia de los servicios secretos y de las informaciones por ellos obtenidas en el marco del proceso penal no pueden aflorar con idéntica naturalidad que un supuesto de investigación policial. En suma, no todos pueden acceder a toda la información con lo que hay elementos sustraídos a una hipotética estrategia defensiva ya sea de un investigado, ya sea respecto de terceros ajenos al procedimiento cuyas comunicaciones o domicilios pudieran verse afectados, que van a permanecer ocultas, lo que puede servir para cuestionar la pureza del procedimiento y de la decisión en torno a las responsabilidades penales.

5. CONCLUSIONES.

Existe una relación concéntrica entre la seguridad nacional y la seguridad pública en tanto ambas trabajan sobre el presupuesto de la existencia de amenazas al Estado de derecho. Sin embargo, los actores habilitados para su protección son distintos, teniendo los servicios secretos competencia sobre la primera y los policiales sobre la segunda. En este sentido, se han establecido herramientas destinadas a conjurar los riesgos anteriormente señalados mediante la atribución de medidas limitativas de derechos fundamentales. En el caso de las agencias de seguridad pública (Policías estatales, autonómicas o locales) sus atribuciones vienen enmarcadas en el ámbito procesal penal con pautas muy rigurosas de conculcación de los derechos mediante la necesidad de una autorización judicial garantista que habilite las actividades invasivas, pero ordenadas, por parte de las fuerzas de seguridad teniendo como marco la LECRIM. El servicio de inteligencia (CNI) sólo de manera relativamente reciente se ha visto apoderado para la interceptación de comunicaciones y la entrada en domicilios mediante una ley de control judicial del año 2002, sin que podamos afirmar que sus exigencias coincidan con las de la LECRIM a la hora de su concesión con lo que nos encontramos con un sistema de doble estándar en función del sujeto actuante.

El concepto de *construcción paralela* resulta de un modo de actuar respecto de las fuerzas policiales quienes reciben información de inteligencia que, por un lado, les permiten construir casos penales pero, por otro, teniendo presente que existe un estándar de obtención rebajado en el caso de la información procedente de inteligencia se ven obligados a ocultar su origen, buscando procedimientos alternativos para evitar que la fuente originaria aflore y permita al investigado cuestionar su obtención mediante la vulneración del proceso debido. Esta cuestión se ha puesto de manifiesto fundamentalmente en Norteamérica fruto de la ruptura del "muro", con los atentados del 11 de septiembre de 2001, entre actividades policiales y de inteligencia que ha provocado la duda respecto del uso de aquellas informaciones que se obtienen del Tribunal de Inteligencia Extranjera (Tribunal FISA) cuyo mandamientos de vigilancia, a una agencia

de inteligencia, suministran informaciones que luego pueden ser empleadas por las fuerzas policiales quienes se han podido ahorrar la justificación de la causa probable ante un órgano judicial para practicar sus investigaciones. Es decir, parece una suerte de atajo operativo que genera dudas, dudas que también nos afectan a nosotros sobre el posible uso de información fruto de una autorización del Juez del TS al CNI fuera una escucha, fuera de una entrada en un domicilio. En este sentido, hay una serie de exigencias que motivarían la comunicación de un hecho delictivo fruto de la práctica de una diligencia restrictiva de derechos fundamentales por nuestro servicio secreto a las agencias policiales que bien pudiera ser la obligación de denuncia general del art. 262 LECRIM. Pero es que una elemental unidad de acción en la prevención de amenazas que afectan conjuntamente a la seguridad pública y nacional obligan a una cooperación entre servicios y la compartición de información. Pensemos en la inminencia de un ataque terrorista del que se tiene conocimiento casualmente por una escucha del servicio secreto, nadie duda de la necesaria comunicación y alerta y ello al margen de la posible clasificación secreta de la información, clasificación que no puede amparar el silencio frente a un hecho delictivo ni dejarlo impune. Para ello, además, existe un proceso de desclasificación.

Nuestro TS ha dicho que cuando un servicio de información extranjero remite una confidencia que sirve para abrir una causa penal, no existe un derecho de conocimiento de la fuente de la fuente, por tanto, no es necesario, ni procedente, ocultar el origen o fuente de conocimiento por la agencia policial. En el supuesto de comunicación por el CNI a una fuerza de seguridad pública también nuestro Alto Tribunal avala, aisladamente eso sí, la comunicación de un hecho delictivo sin entrar en la cuestión de la clasificación o no como secreta de la información, con lo que tampoco parece tener sentido ni la ocultación, ni la elaboración de estrategias alternativas, que pueden llegar a comprometer el procedimiento penal. No cabe, por tanto, *la construcción paralela*, todo ello sin perjuicio que la presencia de los servicios secretos en el proceso penal genera interrogantes que si se quieren despejar exigirá una reforma en el sistema diseñado por la Ley 2/2002 de 6 de mayo.

6. REFERENCIAS BIBLIOGRAFICAS.

Aba Catoira, A. (2020). Rendición de cuentas y servicios de inteligencia. En J. J. Fernández Rodríguez (Ed.), *Seguridad y libertad en el sistema democrático* (pp. 209-237). Tirant lo Blanch.

Alfonso Rodríguez, A. J. (2023). Gobernanza democrática y rendición de cuentas: Control judicial de las actividades de inteligencia (ODS 16.6). *Revista de Derecho UNED*, (31).

Alfonso Rodríguez, A. J. (2024). Interceptación de comunicaciones telefónicas, seguridad(es) y garantías procesales. *Revista Ciencia Policial*, (182).

Arrieta, G. (2025). Balancing the scales: Amici curiae as special masters in the shadow of FISA. *California Western Law Review, 61*(1), Article 6. https://scholarlycommons.law.cwsl.edu/cwlr/vol61/iss1/6

Beck, U. (2006). *La sociedad del riesgo: Hacia una nueva modernidad*. Paidós Ibérica.

Chin, S. (2021). Introducing independence to the Foreign Intelligence Surveillance Court. *The Yale Law Journal, 131*(2). http://www.yalelawjournal.org/author/simon-chin

De la Oliva Santos, A. (2006). *Escritos sobre derecho, justicia y libertad*. Editorial UNAM, Instituto de Investigaciones Jurídicas.

Donohue, L. K. (2021). The evolution and jurisprudence of the Foreign Intelligence Surveillance Court and Foreign Intelligence Surveillance Court of Review. *Harvard National Security Journal, 12*.

Gómez Colomer, J. L. (2006). Adversarial system, proceso acusatorio y principio acusatorio: Una reflexión sobre el modelo de enjuiciamiento criminal aplicado en los Estados Unidos de Norteamérica. *Revista Poder Judicial*, (Especial XIX).

Hassemer, W. (2000). ¿Proceso penal sin protección de datos? En C. M. Romeo Casabona (Ed.), *La insostenible situación del derecho penal* (pp. 103-128). Comares.

Herbón Costas, J. J. (2021). La gestión de las crisis en el marco de la Ley de Seguridad Nacional: La pandemia por covid-19 y la necesidad de una urgente reforma. *Revista Española de Derecho Constitucional, 121*. https://doi.org/10.18042/cepc/redc.121.05

Lanz Muniain, V. (2023). El CNI un servicio de inteligencia y seguridad: Panorama normativo. *Revista Española de Derecho Militar*, (119).

López Alafranca, M. (2014). ¿Pero quién vigilará a los vigilantes? *Revista Cuatrimestral de las Facultades de Derecho y Ciencias Económicas y Empresariales*, (92).

Orgis, M. (2011). Operaciones impulsadas y guiadas por inteligencia: La mejor opción para combatir las amenazas preeminentes. En J. Fernández Rodríguez, D. Sanso-

Rubert Pascual, J. Pulido Grajera, y R. Monsalve (Eds.), *Cuestiones de inteligencia en la sociedad contemporánea* (pp. 143-166). Ministerio de Defensa.

Pascual Sarria, F. (2007). El control judicial a la interceptación de las comunicaciones: Especial referencia al control judicial previo a las intervenciones del Centro Nacional de Inteligencia. *Revista Española de Derecho Militar*, (89).

Pinto Cebrián, F. (2019). *Manual de inteligencia y contrainteligencia (terrorismo y contraterrorismo)*. Amabar.

Reid, L. (2015). NSA and DEA intelligence sharing: Why it is legal and why Reuters and the Good Wife got it wrong. *SMU Law Review, 68*(2), Article 5.

Ruger, T. W. (2007). Chief Justice Rehnquist's appointments to the FISA Court: An empirical perspective. *Northwestern University Law Review, 101*(1).

Sánchez Barrilao, J. F. (2011). Prevención e inteligencia: Centro Nacional de Inteligencia y comunidad de inteligencia ante el terrorismo, la criminalidad organizada y la inmigración ilegal. *Revista Ejército*, (846).

Sánchez Ferro, S. (2020). ¿Misión imposible? Un intento de comprensión jurídica del mundo del espionaje en España. En J. J. Fernández Rodríguez (Ed.), *Seguridad y libertad en el sistema democrático* (pp. 159-207). Tirant lo Blanch.

Sobel, A. X. (2023). Procedural protections in a secret court: FISA amici and expanding appellate review of FISA decisions. *University of Pennsylvania Law Review, 172*. [Nota: Corregido "Pennsilvania" a "Pennsylvania". Faltan números de página o número de artículo.]

Stein, R., Mondale, W., & Fisher, C. (2016). No longer a neutral magistrate: The Foreign Intelligence Surveillance Court in the wake of the war on terror. *Minnesota Law Review, 100*. https://scholarship.law.umn.edu/faculty_articles/564

Zaffaroni, E. R. (2006). *El enemigo en el Derecho Penal*. Dykinson.

ORCID: 0009-0005-2821-4603

Revista Científica del Centro Universitario de la Guardia Civil
Revista Lógos Guardia Civil

II.- TRABAJOS DE INVESTIGACIÓN

Revista Científica del Centro Universitario de la Guardia Civil
Revista Logos Guardia Civil

Artículo de Investigación

ESPAÑA FRENTE A LA DESINFORMACIÓN: DESAFÍOS HÍBRIDOS Y RESPUESTAS CONVENCIONALES

Juan Francisco Adame Hernández
Director de Estrategia, Comunicación y Promoción de Casa Árabe
Máster Universitario en Alta Dirección en Seguridad Internacional
Máster en Estudios Avanzados en Comunicación Política

Recibido 08/04/2025
Aceptado 03/06/2025
Publicado 27/06/2025

Cita recomendada: Adame, J. F. (2025). España frente a la desinformación: desafíos híbridos y respuestas convencionales. *Revista Logos Guardia Civil*, 3(2), pp. 37-70.

Licencia: Este artículo se publica bajo la licencia Creative Commons Atribución-NoComercial-SinDerivadas 4.0 Internacional (CC BY-NC-ND 4.0)
Depósito Legal: M-3619-2023
NIPO en línea: 126-23-019-8
ISSN en línea: 2952-394X

ESPAÑA FRENTE A LA DESINFORMACIÓN: DESAFÍOS HÍBRIDOS Y RESPUESTAS CONVENCIONALES

Sumario: 1. INTRODUCCIÓN. 2. DESINFORMACIÓN, POSVERDAD Y FAKE NEWS. 2.1. Conceptos y definiciones. 3. ESTRATEGIAS HÍBRIDAS Y ZONA GRIS. 3.1. Manipulación e interferencia de información extranjera (FIMI). 4. DOMINIO COGNITIVO Y DESINFORMACIÓN. 5. CONSTRUCCIÓN DE NARRATIVAS Y MARCOS. 5.1. Implementación. 5.2. Impacto de las Narrativas y los Marcos en el Dominio Cognitivo. 6. EVOLUCIÓN DE LA DESINFORMACIÓN. 7. MEDIDAS Y HERRAMIENTAS ACTUALES PARA COMBATIR LA DESINFORMACIÓN EN ESPAÑA. 7.1. Procedimiento de Actuación contra la Desinformación. 8 CONCLUSIONES. 9 REFERENCIAS BIBLIOGRÁFICAS.

Resumen: En el actual entorno geopolítico, caracterizado por la proliferación de tecnologías de la información y la interconexión global, **la desinformación se ha consolidado como una amenaza multidimensional** que compromete las estructuras de seguridad nacional y la cohesión social de los Estados. Este artículo analiza **la respuesta institucional y estratégica de España frente a la desinformación**, enmarcándola dentro del contexto más amplio de las estrategias híbridas y de la **interferencia y manipulación informativa extranjera (FIMI)**.

El estudio aborda conceptos clave como *desinformación*, *posverdad* y *zona gris*, vinculándolos con la **evolución doctrinal de las estrategias híbridas en el seno de la Unión Europea**. Se presta especial atención al **dominio cognitivo** y a los mecanismos de construcción de narrativas y marcos interpretativos empleados para moldear y distorsionar la percepción pública. La última sección ofrece una **evaluación crítica de las principales medidas adoptadas por España para contrarrestar la desinformación**, valorando su coherencia, aplicación y eficacia en un panorama de amenazas en constante transformación.

Abstract: In today's geopolitical environment—marked by the proliferation of information technologies and global interconnectedness—**disinformation has emerged as a multidimensional threat** to national security structures and the social cohesion of states. This article analyzes **Spain's institutional and strategic response to disinformation**, situating it within the broader framework of hybrid strategies and **foreign information manipulation and interference (FIMI)**.

The study first clarifies key concepts such as *disinformation*, *post-truth*, and the *grey zone*, linking them to the **doctrinal evolution of hybrid threats in the European Union**. Particular attention is paid to the **cognitive domain** and the ways in which narrative construction and framing mechanisms are used to shape and distort public perception. The final section provides a **critical assessment of the main counter-disinformation measures adopted by Spain**, evaluating their coherence, implementation, and overall effectiveness in the face of a rapidly evolving threat landscape.

Palabras clave: Desinformación, *Fake news*, Estrategias híbridas, Dominio cognitivo, Narrativas.

Keywords: Disinformation, Fake news, Hybrid strategies, Cognitive domain, Narratives.

ABREVIATURAS

CIS: Centro de Investigaciones Sociológicas

CNI: Centro Nacional de Inteligencia

DESI: Digital Economy and Society Index

DSN: Departamento de Seguridad Nacional

EEAS/SEAE: European External Action Service/Servicio Europeo de Acción Exterior

ELISA: Estudio Simplificado de Fuentes Abiertas

ENISA: Unión Europea para la Ciberseguridad

ESN: Estrategia de Seguridad Nacional

EU/UE: Unión Europea

FIMI: Foreign Information Manipulation and Interference (Manipulación e Interferencia de Información Extranjera)

FIP: Federación Internacional de Periodistas

INCIBE: Instituto Nacional de Ciberseguridad es ciberseguridad

MAEUEC: Ministerio de Asuntos Exteriores, Unión Europea y Cooperación

MPJRC: Ministerio de la Presidencia, Justicia y Relaciones de las Cortes

OMS: Organización Mundial de la Salud

OTAN/NATO: Organización del Tratado del Atlántico Norte/North Atlantic Treaty Organization

1. INTRODUCCIÓN

En la era digital actual, marcada por la rápida difusión de información a través de las redes sociales y las tecnologías de la comunicación, la desinformación se ha convertido en una amenaza estratégica de primer orden. Este fenómeno, que incluye las noticias falsas (*fake news*) y la posverdad, ha adquirido una relevancia sin precedentes en el ámbito geopolítico, afectando tanto la estabilidad de los sistemas políticos como la percepción pública y la seguridad nacional. España no ha sido ajena a estos desafíos, enfrentándose a campañas de desinformación que, en muchos casos, han sido utilizadas como herramientas dentro de estrategias híbridas más amplias.

A menudo se interpreta la desinformación como un fenómeno en sí mismo o se aborda de una manera aislada o descontextualizada (Lazer et al., 2018). Se relativiza, se abstrae o se obvian las estrategias en las que la desinformación está inserta (MAEUEC, 2021). Obviando el necesario enfoque multidisciplinar (Wardle y Derakhshan, 2017) o la necesidad de identificar los objetivos estratégicos que estas acciones o campañas de desinformación persiguen (Terán, 2019). Incluso cuando hay una referencia a las estrategias híbridas y/o a la zona gris, habitualmente no suele abordarse en profundidad, quedando relegado a la mera mención (DSN, 2021). La desinformación, lejos de ser un fenómeno aislado, se inserta dentro de un marco estratégico más amplio, incluyendo las estrategias híbridas y la llamada "zona gris" (OTAN, 2024) y especialmente en la Manipulación e interferencia de información extranjera (FIMI, *Foreign Information Manipulation and Interference*).

2. DESINFORMACIÓN, POSVERDAD Y FAKE NEWS

La desinformación, no es un fenómeno reciente (Allcott y Gentzkow, 2017; Tandoc, Lim & Ling, 2018). Desde que las sociedades comenzaron a organizarse en estructuras jerárquicas, los seres humanos han fabricado y difundido deliberadamente historias incorrectas y engañosas (Burkhardt, 2017). Desde las tácticas de difamación política en la Antigua Roma hasta las estrategias de propaganda durante la Primera y Segunda Guerra Mundial (Posetti y Matthews, 2018), la desinformación ha sido utilizada para manipular y convencer a otros. La desinformación ha alcanzado niveles sin precedentes, alterando no solo la percepción pública, sino también influyendo directamente en procesos políticos y sociales a nivel global. Sin embargo, como repasan Julie Posetti y Alice Matthews en su compilación "*A Short Guide to History of Fake News and Disinformation*" (2018), la fabricación y manipulación de la información no es un fenómeno nuevo.

En los últimos años los medios de comunicación, las campañas políticas o los debates deportivos (o extradeportivos) en redes sociales se han llenado de nuevos conceptos como noticias falsas o *fake news* (Tandoc, Lim & Ling, 2018), la posverdad (McIntyre, 2018) o la *disinformation/misinformation* (Comisión Europea, 2022). Ha ganado relevancia pública debido a una serie de sucesos internacionales, como lo sucedido con el mundial de Qatar (Newtral, 2022), el escándalo de Cambridge Analytica (Chan, 2020) o lo sucedido en las elecciones presidenciales de Estados Unidos (BBC Mundo, 2018); lo que ha reavivado el debate sobre sus implicaciones para los sistemas democráticos, la percepción pública y los intereses geopolíticos de ciertos países. Es un debate recurrente, donde suelen destacarse el papel de las redes sociales, los medios de comunicación tradicionales, los verificadores o la ciberseguridad. Esta realidad

polisémica, confusa y a menudo ambigua agrupa diferentes conceptos que intentan nombrar, explicar o aludir diferentes realidades.

2.1. CONCEPTOS Y DEFINICIONES

La desinformación, las *fake news* o la posverdad son términos, palabras y conceptos que se han popularizado mucho, pasando a formar parte del habla coloquial y habitualmente usándose como sinónimos para intentar reflejar una realidad habitualmente diferente y compleja. Sin embargo, aunque estos términos se utilizan frecuentemente de manera intercambiable, cada uno tiene matices y características específicas que los distinguen, lo que es crucial para una comprensión más profunda del fenómeno (DSN, 2022).

Tabla 1

Concepto	Definición	Relación con la verdad
Fake News	Noticias inventadas sin base real	Falsa completamente
Posverdad	Cuando importan más las emociones que los hechos	Lo emocional prima sobre lo verdadero
Desinformación	Información falsa o manipulada difundida deliberadamente con fines estratégicos	Mezcla verdades y falsedades para generar un efecto concreto

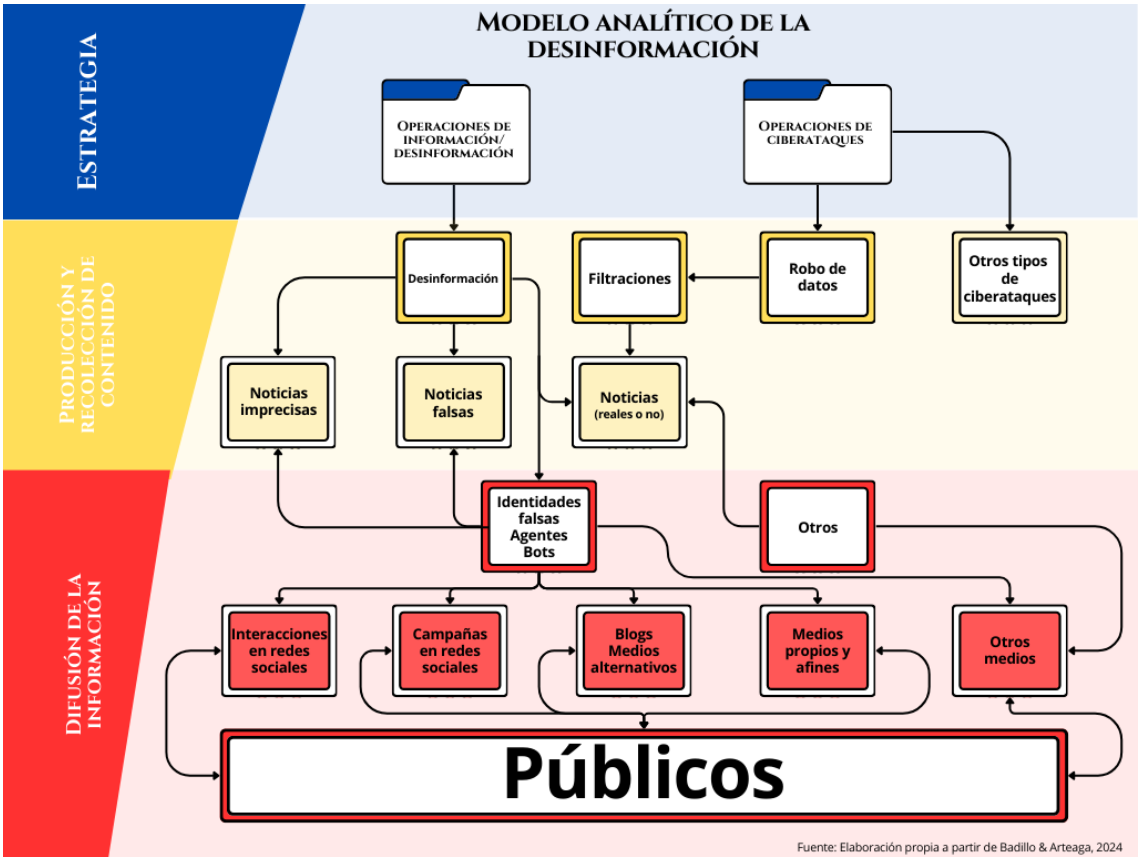
Fuente: Elaboración propia

Empecemos desenmarañando esta compleja mescolanza temática por el aspecto más sencillo, las *fake news* o noticias falsas. Entendemos como *fake news* aquellas noticias falsas e inventadas[1] (Gelfert, 2018). Estas noticias no solo son fabricadas sin ninguna base en la realidad, sino que a menudo son diseñadas para parecer plausibles y manipular a la audiencia, explotando emociones y prejuicios para maximizar su impacto (DSN, 2022)[2]. Son supuestas noticias creadas desde la fantasía (dado que no tiene una relación con la realidad). Apoyándonos en la tabla 1, quizás es más fácil definirlas por oposición, no son ni noticias reales pero descontextualizadas ni noticias exageradas (de nuevo reales) ni noticas inexactas (con elementos reales) (DSN, 2023a). Es fundamental diferenciar las *fake news* de otros tipos de información incorrecta, como las noticias descontextualizadas o exageradas, ya que estas últimas, aunque potencialmente engañosas, están basadas en hechos reales, lo que las distingue de las noticias completamente fabricadas (DSN, 2022). Especialmente útil el modelo analítico de la desinformación propuesto por Badillo y Arteaga (2024) recogido en la Figura 1.

[1] No obstante, no es un término pacificado (Carson, 2018), y aunque se puede ver una evolución hacia la diferenciación conceptual hay autores (Flores, 2022) y especialmente en el mundo periodístico (FIP, 2018), donde llegan a presentarse "argumentos" como que el mero hecho de que algo sea falso lo invalida para ser noticia (Mayoral, Parratt & Morata, 2019).

[2] El uso de la inteligencia artificial ha amplificado esta capacidad, permitiendo la creación de *deepfakes* y otros tipos de contenido manipulado que pueden ser distribuidos masivamente con gran rapidez y alcance (DSN, 2023a).

Figura 1



La posverdad[3] es un fenómeno multifacético (Caridad-Sebastián et al, 2018), donde es más relevante su verosimilitud (Rodrigo Alsina, 2005), que sea creíble, con independencia de los hechos ciertos o reales (Dahlgren, 2018). En la posverdad, las emociones y creencias personales prevalecen sobre los hechos objetivos, lo que tiene profundas implicaciones para la democracia y la cohesión social, ya que permite que narrativas emotivas y, a menudo, engañosas se impongan en el discurso público (DSN, 2022; DSN, 2024). Este fenómeno no solo altera la percepción individual, sino que también facilita la creación de "cámaras de eco"[4] en las que las personas son expuestas repetidamente a las mismas ideas, reforzando sus creencias y aislándolas de otras perspectivas (DSN, 2023a).

Sobre desinformación también hay múltiples definiciones, que han ido mutando con el paso del tiempo y en función del sector o ámbito donde se emplean o se esbozan (Arteaga, 2020). Este término abarca no solo la difusión intencional de información falsa, sino también la manipulación sutil de hechos para distorsionar la realidad y confundir al

[3] No hay una posición única, pero a diferencia del concepto anterior (y de matices), hay un consenso mayoritario en el elemento central de "querer creer" por encima de los hechos o la realidad (Olmo, 2019). El fenómeno, "Es mentira, pero podría ser verdad" https://twitter.com/hematocritico/status/1241797239779069952?lang=es

[4] Una cámara de eco, o *echo chamber* en inglés, es un fenómeno en el que la información, opiniones y creencias se refuerzan y amplifican dentro de un grupo o comunidad cerrada, limitando la exposición a perspectivas diferentes (Jamieson y Cappella, 2008). Para más información sobre las cámaras de eco consultar: *The echo chamber is overstated* (Dubois y Blank, 2018). https://www.tandfonline.com/doi/full/10.1080/1369118X.2018.1428656#abstract

público (DSN, 2022). El DSN, alineándose con los postulados de la UE, la define como "*Se considera desinformación a la información verificablemente falsa o engañosa que se crea, presenta y divulga con fines lucrativos o para inducir a error deliberadamente a la población, y que puede causar un perjuicio público*" (DSN, 2022, p.253).

Aunque adecuada, esta definición restringe o minimiza algunos de los elementos que si se señalan en la Estrategia de Seguridad Nacional[5] como la referencia al ámbito cognitivo (DSN, 2021) o el énfasis en la intencionalidad y los objetivos de quienes llevan a cabo las campañas de desinformación (dotándolo así de un contexto). El impacto cognitivo de la desinformación es crucial, ya que no solo se trata de difundir información falsa, sino de alterar la percepción y el juicio del público, erosionando la confianza en las instituciones y fomentando la polarización social (DSN, 2022; DSN, 2023a). Opinión coincidente con otros autores como Artega u Olmo que señalan que "La desinformación permite fragmentar, aislar y manipular las opiniones públicas infectadas, desacreditar y cuestionar los hechos objetivos y acreditar como reales las emociones virtuales y las percepciones inducidas" (Artega, 2020) y "cuando la falsedad se vuelve más sutil, más compleja, ha sido creada con una intencionalidad táctica, responde a una estrategia y persigue objetivos, es cuando podemos hablar desinformación" (Olmo, 2019).

3. ESTRATEGIAS HÍBRIDAS Y ZONA GRIS

Las estrategias híbridas se definen como un enfoque de conflicto que combina elementos convencionales y no convencionales, utilizando una variedad de herramientas —militares, económicas, diplomáticas, cibernéticas y de información— para lograr objetivos estratégicos (Colom, 2018). Estas herramientas incluyen no solo la manipulación directa de la información, sino también la creación de narrativas que modifiquen la percepción pública en el largo plazo, una característica central tanto de las operaciones de influencia como de la desinformación (Torres Soriano, 2022). El uso de estas estrategias se justifica por su capacidad para explotar vulnerabilidades a través de un enfoque que integra lo militar con otros dominios, como el cognitivo y el informativo, creando una sinergia que multiplica su efectividad en contextos de baja intensidad (Walker, 1998).

La zona gris, por su parte, se caracteriza por la aplicación de tácticas diseñadas para permanecer por debajo del umbral que desencadenaría una guerra abierta. Este concepto es fundamental para comprender cómo los actores estatales y no estatales desafían el orden internacional sin cruzar las líneas rojas que llevarían a un conflicto armado (Martín Renedo, 2022). En la práctica, las operaciones en la zona gris incluyen desde la coerción económica y el uso de desinformación hasta el empleo de fuerzas especiales en misiones encubiertas, las cuales están diseñadas para ser difíciles de atribuir directamente a un Estado (McCuen, 2008). El solapamiento entre el plano físico, virtual y cognitivo en la zona gris permite la ejecución de estas estrategias de manera más efectiva, ya que la percepción del conflicto es manipulada para desorientar a las poblaciones objetivo y debilitar su capacidad de respuesta (Lupiáñez Lupiáñez, 2023).

[5] Aunque esta definición es precisa, es importante considerar que la desinformación también puede ser motivada por otros objetivos no políticos o ideológicos, como es el crimen organizado o la búsqueda de lucro de actores no estatales (DSN, 2023a; Marchal González, 2023).

Las estrategias híbridas[6] y la "zona gris" es una evolución de tácticas y estrategias históricas de guerra irregular, ahora potenciadas por la tecnología moderna y las redes de información, lo que permite una influencia más efectiva y menos detectable en un contexto global (Hafen, 2024). La desinformación, la propaganda y las operaciones de influencia son componentes esenciales de estas estrategias, que se despliegan en un entorno cada vez más complejo y globalizado (Hoffman, 2009).

La propaganda moderna va más allá de la simple difusión de mensajes; se trata de una manipulación sofisticada de la información para moldear percepciones y comportamientos en línea con los intereses estratégicos de quienes la promueven (Calvo Albero, 2017). La propaganda[7] puede ser vista como una extensión de las operaciones psicológicas, donde no solo se busca influir en la opinión pública, sino también desmoralizar al adversario y alterar su capacidad de decisión (Rid, 2021)[8]. Desde 2023, este tipo de operaciones se ha visto intensificado, especialmente en el contexto de conflictos globales como los ocurridos en Ucrania y Gaza, donde la propaganda ha jugado un papel crucial en la polarización de las opiniones públicas y la manipulación de la información a escala internacional (DSN, 2024)

En este contexto, la desinformación no solo actúa como una herramienta de influencia, sino que también facilita otras operaciones híbridas al debilitar la cohesión social y la confianza en las instituciones, creando un entorno propicio para la implementación de tácticas más agresivas sin necesidad de un enfrentamiento militar abierto (Alastuey Rivas et al, 2024). Es crucial comprender que las estrategias híbridas no son un fenómeno nuevo, sino una evolución de las tácticas de guerra irregular que han sido empleadas a lo largo de la historia, aunque los cambios sociales y el avance de la tecnología han ampliado enormemente las herramientas disponibles para estas estrategias, permitiendo su aplicación en una escala global y con un impacto significativo en la estabilidad internacional (Calvo, 2023). Esto se puede observar con nitidez en la Doctrina Primakov/Gerasimov rusa, en la concepción las "Tres Guerras" de China o en la "Nueva Conceptualización de la Zona Gris" occidental (Adame Hernández, 2024).

3.1. MANIPULACIÓN E INTERFERENCIA DE INFORMACIÓN EXTRANJERA (FIMI)

El concepto de Manipulación e interferencia de información extranjera (FIMI, *Foreign Information Manipulation and Interference*) hace referencia a las actividades deliberadas llevadas a cabo por actores extranjeros con el objetivo de distorsionar la información, manipular la percepción pública e influir en procesos políticos y sociales en otros países. Según el informe conjunto de la Agencia de la Unión Europea para la Ciberseguridad (ENISA) y el Servicio Europeo de Acción Exterior (SEAE), FIMI abarca una variedad de acciones que incluyen la difusión de desinformación, propaganda y operaciones psicológicas que buscan sembrar discordia y desestabilizar sociedades democráticas

[6] A pesar de que el concepto de "guerra híbrida" ha sido objeto de múltiples definiciones y debates, persiste una falta de consenso sobre su caracterización precisa, lo que complica su estudio y aplicación en el análisis estratégico contemporáneo (Colom, 2018b).

[7] Específicamente, la propaganda se define como un "conjunto de técnicas utilizadas, de modo sistemático, para expandir opiniones o ideas parciales o sesgadas entre la masa, con una intención propia, a menudo, política" (Donoso Rodríguez, 2020, p. 30) lo que la convierte en una herramienta clave en las operaciones psicológicas.

(ENISA & SEAE, 2022). La FIMI también puede involucrar la manipulación de narrativas culturales e históricas para avivar conflictos internos y desestabilizar el orden social, explotando temas sensibles que resuenan con los prejuicios o miedos existentes en una sociedad (Buvarp, 2021). La sofisticación de estas operaciones radica en su capacidad para aprovechar grietas preexistentes dentro de las sociedades objetivo, exacerbando divisiones y provocando reacciones que socavan la cohesión social y política (Allenby y Garreau, 2017). Estas actividades pueden tener consecuencias profundas para la estabilidad de las instituciones democráticas, ya que se enfocan en explotar las vulnerabilidades sociales y políticas (ENISA & SEAE, 2022).

En el contexto de FIMI, es esencial reconocer que estas operaciones no siempre involucran la difusión de información completamente falsa. A menudo, se basan en distorsiones sutiles de hechos reales, el empleo de técnicas como la saturación de la información o la creación de burbujas informativas (Rid, 2021); lo que dificulta la detección y la respuesta. Estas estrategias, denominadas como "manipulación sutil de la verdad", es particularmente peligrosa ya que juega con la percepción pública y la credibilidad de las fuentes informativas (Castro Torres, 2021). Además, la manipulación de la información a través de canales no tradicionales, como las redes sociales y plataformas de mensajería instantánea, permite a los actores extranjeros maximizar el impacto de sus campañas al aprovechar las características virales y el alcance global de estas herramientas (EEAS, 2024).

FIMI se enmarca dentro de las estrategias híbridas. La propaganda y las acciones de influencia son herramientas clave dentro del marco de FIMI. La propaganda es empleada para promover narrativas que favorecen los intereses del actor extranjero, utilizando medios de comunicación controlados o afines para diseminar mensajes específicos. Estas narrativas son diseñadas cuidadosamente para parecer legítimas y a menudo se apoyan en fuentes parciales o sesgadas que otorgan credibilidad a los mensajes difundidos (Maggioni y Magri, 2015). Narrativas ideadas para generar desconfianza hacia las instituciones democráticas y polarizar a la sociedad (Bennett & Livingston, 2020). Además, las acciones de influencia se dirigen a moldear la opinión pública o influir en decisiones políticas, lo que puede incluir desde la manipulación de redes sociales hasta la financiación encubierta de actores políticos o mediáticos en el país objetivo (SEAE, 2023). Un ejemplo reciente de este proceder se ha observado en las elecciones presidenciales rumanas (Comisión Europea, 2024). El anonimato que brindan las plataformas digitales y la posibilidad de operar a través de intermediarios o *proxies* añade una capa de complejidad a la hora de rastrear e identificar a los verdaderos perpetradores de estas campañas, lo que dificulta la implementación de contramedidas efectivas (Castro Torres, 2021). El uso de estos métodos ha permitido a los actores extranjeros operar con una capa adicional de anonimato y denegabilidad, complicando los esfuerzos para identificar y contrarrestar estas actividades (DSN, 2024).

4. DOMINIO COGNITIVO Y DESINFORMACIÓN

Aunque la conceptualización del dominio cognitivo es relativamente moderna, las estrategias para operar sobre él como la propaganda (Calvo, 2023), las acciones de influencia (Jordán, 2018) y desestabilización (Quiñones de la Iglesia, 2021) no lo son. Estas tácticas han sido históricamente utilizadas en diversos contextos geopolíticos, evolucionando con el tiempo para adaptarse a las nuevas tecnologías de la información y las cambiantes dinámicas sociales. Por ejemplo, la propaganda, que alguna vez dependió

exclusivamente de medios tradicionales como la prensa y la radio, ahora se dispersa a través de plataformas digitales y redes sociales, permitiendo una mayor penetración y rapidez en la difusión de mensajes. Estas herramientas han adquirido una sofisticación sin precedentes, aprovechando la velocidad y el alcance de Internet y las redes sociales para amplificar sus efectos, como se observa en las tácticas empleadas por grupos como Al Qaeda y el Estado Islámico, que han usado estas tecnologías para influir en la opinión pública global y legitimar sus acciones (Astorga González, 2020). La influencia de las plataformas digitales es tal que permiten a los actores malintencionados segmentar audiencias y personalizar mensajes, creando cámaras de eco que refuerzan creencias preexistentes y dificultan la diseminación de información contraria. Esto se potencia con el uso de algoritmos que favorecen la polarización al priorizar contenido sensacionalista y emocionalmente cargado, lo que, a su vez, facilita la manipulación del dominio cognitivo a gran escala (DSN, 2023b).

La teoría estructuralista de Louis Althusser sobre la construcción ideológica, donde los medios de comunicación juegan un rol central en la creación y mantenimiento de las ideologías que dominan la percepción pública, refuerza la comprensión de cómo las tácticas de desinformación se insertan en el dominio cognitivo[9] (Althusser, 1971). En consonancia con esto, la manipulación del dominio cognitivo implica la creación de realidades percibidas que, aunque no necesariamente reflejen la realidad objetiva, se convierten en la base sobre la cual se toman decisiones políticas y sociales (Lupiáñez Lupiáñez, 2023). Como apuntan diversos autores como Foucault, el lenguaje no solo describe el mundo, sino que actúa sobre él (Foucault, 1972), lo que refuerza la idea de que el dominio cognitivo puede ser manipulado a través de la construcción de narrativas que reconfiguran la realidad percibida.

En relación a la desinformación, la zona gris se enfocará principalmente en establecer el contexto, utilizando estrategias como la propaganda o la desinformación, con el objetivo de obtener gradualmente una ventaja estratégica sobre el oponente, lo que facilitaría mejorar la eficacia de futuras intervenciones (Hernández-García, 2022). Libicki refuerza esta idea al explicar cómo las operaciones cognitivas no siempre buscan resultados inmediatos, sino que pueden estar diseñadas para sembrar dudas y confusión, afectando a largo plazo la capacidad de un adversario para tomar decisiones efectivas (Libicki, 2021). Este enfoque subraya la importancia de la gradualidad en la estrategia de desinformación, donde los pequeños cambios en la percepción y la narrativa pueden culminar en una alteración significativa de la realidad percibida, haciendo que el oponente pierda la iniciativa y el control sobre la situación. Destacar en esta aproximación la concurrencia entre objetivos, visión estratégica y gradualidad.

La relación entre la manipulación cognitiva y los conflictos políticos también se puede analizar desde la perspectiva clausewitziana. Clausewitz argumenta que la guerra es un acto político racional donde se busca desmoralizar al adversario no solo a través del conflicto directo, sino también manipulando las pasiones de la población y la percepción

[9] La doctrina militar española subraya la relevancia de STRATCOM (*Strategic Communications*, Comunicación Estratégica) como una función directiva que integra INFOOPS (*Information Operations*. Operaciones de Información) y PSYOPS (*Psychological Operations*. Operaciones Psicológicas), aplicando técnicas de ingeniería social y comunicación estratégica para moldear el entorno informativo y cognitivo. Estas capacidades permiten a las Fuerzas Armadas alcanzar objetivos que trascienden los medios convencionales, operando en un ámbito intangible que impregna todos los demás dominios (PDC-01, 2018).

de la realidad (Clausewitz, 1976). A través de la desinformación es posible erosionar la moral tanto de un ejército enemigo como, de manera aún más significativa, de su población, con el propósito de persuadir a sus decisores políticos para que detengan su actitud beligerante, propiciar una negociación u obtener beneficios en una ya prevista (Rodríguez Lorenzo et al, 2023).

Un factor fundamental a considerar y que no suele atenderse más que de manera colateral es la relación y afectación política. Este aspecto, aunque crucial, a menudo se subestima en los análisis sobre desinformación, donde se pone mayor énfasis en los aspectos técnicos o tácticos, dejando de lado las implicaciones más amplias para la gobernanza y la estabilidad política. En una lógica clausewitziana, "si la guerra es de naturaleza política, resulta evidente que el objetivo principal no son las fuerzas armadas enemigas, sino el liderazgo político" (Calvo Albero, 2017).

Es la intersección entre la desinformación utilizada en las estrategias híbridas y de zona gris; con los objetivos perseguidos (especialmente la afectación política) donde conectan con la sociedad, la agenda y opinión pública (Sartori, 2007). En este contexto, la manipulación de la información y la creación de narrativas alternativas no solo impactan a nivel estatal o militar, sino que también tienen profundas implicaciones en el tejido social y cultural. La construcción de estos relatos, que utilizan el cine y los medios[10] como herramientas de manipulación emocional, sigue siendo fundamental para comprender cómo las narrativas malintencionadas pueden dividir y confundir a la sociedad (Davis, 2005). La capacidad de estas estrategias para modificar la percepción pública no solo se debe a la sofisticación de las tácticas empleadas, sino también a la manera en que estas narrativas se alinean con las preocupaciones y miedos existentes en la sociedad, amplificándolos y redirigiéndolos contra objetivos específicos (Castro Torres, 2021).

La construcción de relatos malintencionados, que buscan dividir y confundir a la sociedad, se convierte en una herramienta poderosa para desestabilizar no solo a los gobiernos, sino también a las comunidades y a la cohesión social en su conjunto. La necesidad de crear un relato malintencionado que pueda ser explotado en beneficio propio (Rodríguez Lorenzo et al, 2023), una narrativa atractiva que sustente la estrategia híbrida (Torres, 2022) y la ineludible generación de un relato que auspicie, cubra, fortalezca y ampare la zona gris (Hernández-García, 2022); otorgan un gran papel a los marcos cognitivos (Goffman, 2006), la comunicación persuasiva (Candelas, 2023) y opinión pública (Sartori 2007). Estos elementos, aunque subestimados en muchos análisis, son fundamentales para entender cómo la desinformación se inserta en el tejido social y se convierte en una fuerza de cambio, erosionando la confianza en las instituciones y alterando la percepción de la realidad. Entender la relación entre la manipulación cognitiva y los cambios sociales es crucial, ya que, como lo describe Berger y Luckmann (2003), la construcción social de la realidad es un proceso dinámico (externalización, objetivación e internalización) que puede ser fácilmente influenciado por actores con el control sobre los medios (interacción social) y las narrativas (lenguaje).

[10] Un ejemplo muy elocuente es el uso de la comunicación más tradicional (como el cine) y la comunicación digital (videos con alto nivel de calidad y producción difundidos *online*) en las estrategias de comunicación de organizaciones tan poco "occidentales" como *Daesh*. Con el uso, además de aspectos técnicos, de tácticas emocionales y la explotación de sesgos cognitivos como el anclaje se han convertido en componentes clave para moldear la percepción del conflicto (Astorga González, 2020).

5. CONSTRUCCIÓN DE NARRATIVAS Y MARCOS

Las narrativas son relatos estructurados que buscan dar sentido a los eventos y moldear la percepción del público. Desde la antigüedad, la propaganda se ha basado en la construcción de relatos que moldean la percepción pública. Se ha descrito cómo se crean "ilusiones necesarias"[11] para que ciertos grupos de poder mantengan su influencia sobre la sociedad (Herman & Chomsky, 1988). En el contexto de la desinformación moderna, las narrativas son diseñadas no solo para convencer, sino para arraigar creencias que son difíciles de erradicar incluso cuando se exponen como falsas[12]. Flynn, Nyhan y Reifler (2017) identifican que las percepciones erróneas políticas no son simples fallos de información, si no que se deben a percepciones erróneas (creencias falsas o infundadas sostenidas con confianza y con resistencia a la corrección), a factores individuales (como los sesgos cognitivos o las identidades partidistas o ideológicas) y a la resistencia al cambio (pasee a la constatación de información falsa o procesos de verificación o fact-checking); pero también entorno al mediático y político (facilitando la exposición selectiva a fuentes).

Estas narrativas, una vez instauradas, pueden seguir ejerciendo un efecto duradero debido a la inercia cognitiva y la resistencia al cambio de las creencias establecidas (Libicki, 2021; Flynn, Nyhan, & Reifler, 2017). Las narrativas falsas y altamente engañosas tienden a prevalecer debido a su capacidad para explotar las emociones humanas, como el miedo y la indignación moral, lo que aumenta su impacto y difusión en redes sociales (Pennycook & Rand, 2021).

El concepto de "marco" o *framing* se refiere a las estructuras cognitivas que determinan cómo interpretamos y comprendemos la información. Estos marcos actúan como atajos mentales que organizan la información y nos permiten interpretar los hechos según esquemas previos de significado. La teoría de los marcos cognitivos destaca cómo las estructuras de interpretación que utiliza la sociedad para dar sentido a los eventos pueden ser manipuladas a través de la comunicación persuasiva (Goffman, 2006). La disputa por el control de estos marcos se ha convertido en un elemento central en la lucha contra la desinformación, el *framing* no solo busca combatir las falsedades, sino también establecer marcos alternativos que reconfiguren el debate público (Tuñón Navarro, Oleart, & Bouza García, 2019). En el contexto de las estrategias híbridas, y por extensión del dominio cognitivo, los marcos son utilizados para enfocar la atención del público en ciertos aspectos de la realidad mientras se ocultan o distorsionan otros[13]. Este proceso permite que ciertos relatos prevalezcan, no por su veracidad, sino por la manera en que se presentan y contextualizan. Este proceso es clave para mantener el control narrativo y

[11] En la obra Manufacturing Consent: The Political Economy of the Mass Media (Herman & Chomsky, 1988), la expresión " ilusiones necesarias" no se encuentra como una cita textual. Sin embargo, el concepto se desarrolla a lo largo de la misma. El concepto "*necessary illusions*" proviene de la obra posterior de Ilusiones necesarias (Chomsky, 1992).

[12] De acuerdo con investigaciones recientes, la susceptibilidad a la desinformación no está únicamente impulsada por el partidismo, sino también por la falta de razonamiento cuidadoso y el uso de heurísticas, como la familiaridad con la información y la credibilidad de la fuente (Pennycook et al, 2021).

[13] Las investigaciones sugieren que la interacción entre las redes sociales y la psicología humana, en particular la tendencia a usar atajos mentales y a depender de la familiaridad, contribuye significativamente a la propagación y persistencia de las noticias falsas (Pennycook et al, 2021).

evitar que se cuestionen las premisas fundamentales de las acciones emprendidas en un conflicto (Colom, 2018).

En la práctica moderna, el *framing* se ha convertido en una herramienta clave no solo para moldear la interpretación de los eventos, sino también para influir en las emociones del público, explotando sesgos cognitivos que dificultan la reflexión crítica (Astorga González, 2020).

5.1. IMPLEMENTACIÓN

La construcción de narrativas y marcos en el contexto de la desinformación implica un proceso complejo donde se crean relatos y estructuras cognitivas diseñadas para influir en la percepción pública de manera profunda y duradera. Este proceso se basa en una comprensión avanzada de las ciencias del comportamiento, donde se explotan sesgos cognitivos como el de anclaje, la disponibilidad y la confirmación para asegurar que las narrativas construidas sean resistentes al cambio (Astorga González, 2020). La sofisticación en la construcción de estas narrativas emplea la capacidad para combinar hechos reales con distorsiones sutiles, haciendo que sean más difíciles de desacreditar y más fáciles de aceptar por la audiencia (Rid, 2021). De esta manera, las narrativas, que explotan los sesgos cognitivos y emocionales del público, se estructuran para ser simplificadas y emocionales, lo que aumenta su efectividad en la manipulación mediática (Herman & Chomsky, 1988). Estas narrativas no solo buscan convencer, sino también establecer una percepción de la realidad resistente a la corrección, incluso cuando se expone su falsedad[14]. La exposición repetida a noticias falsas aumenta su credibilidad percibida, incluso cuando estas son inicialmente plausibles. Este efecto, conocido como la "ilusión de verdad", juega un papel crucial en la permanencia y aceptación de las narrativas falsas (Pennycook et al, 2021).

Además, el *microtargeting* o segmentación de la población según sus creencias y valores ha permitido que los mensajes se adapten específicamente a cada grupo, unido a la proliferación de medios y canales alternativos (y en ocasiones opacos a la mayoría de la población y a la opinión pública) ha amplificado la capacidad de estos marcos para influir en la percepción pública aumentando la efectividad de la manipulación (Astorga González, 2020). Este enfoque personalizado en la difusión de desinformación permite maximizar el impacto en diferentes segmentos de la sociedad, fomentando la polarización y reforzando creencias preexistentes mientras que dificulta su detección (Maggioni y Magri, 2015).

El impacto de estas narrativas y marcos es tal que, incluso cuando se desacreditan, pueden seguir influyendo en la opinión pública debido a la inercia cognitiva, un fenómeno en el que las creencias previamente establecidas son resistentes al cambio (Libicki, 2021). Esto es particularmente evidente en la manera en que ciertos marcos narrativos persisten en el discurso público mucho después de que se ha demostrado su falsedad, continuando su influencia en la percepción y la acción social (Juurvee y Mattiisen, 2020). De este modo, la construcción de narrativas y marcos se convierte en una herramienta poderosa

[14] Otro ejemplo sería la “guerra memética”, que utiliza memes y otras formas de desinformación viral, busca crear y difundir narrativas que alteran las percepciones y emociones del público objetivo, logrando un impacto duradero y difícil de contrarrestar, especialmente cuando se trata de contenido paródico y de fuentes civiles (Arias Gil, 2019).

para moldear la percepción pública y mantener el control sobre la interpretación de la realidad.

5.2. IMPACTO DE LAS NARRATIVAS Y LOS MARCOS EN EL DOMINIO COGNITIVO

Las narrativas y los marcos tienen un impacto profundo en el dominio cognitivo, moldeando no solo cómo se perciben los eventos, sino también cómo se entienden y recuerdan. Se ha destacado que la creación de un relato malintencionado puede ser explotado en beneficio de aquellos que controlan la narrativa, otorgando un gran poder a los marcos cognitivos y la comunicación persuasiva (Rodríguez Lorenzo et al, 2023; Torres, 2022). Estos elementos son fundamentales para entender cómo la desinformación se inserta en el tejido social y se convierte en una fuerza de cambio, erosionando la confianza en las instituciones y alterando la percepción de la realidad. Además, estos marcos no solo influyen en la percepción individual, sino que también afectan la memoria colectiva, condicionando la forma en que las sociedades recuerdan y aprenden de los eventos históricos, lo cual puede tener repercusiones a largo plazo en la cohesión social y en la formación de identidades nacionales (Aznar Fernández-Montesinos, 2021). La propaganda y la desinformación no solo operan a través de mensajes directos, sino que también configuran el entorno cognitivo en el que se interpretan estos mensajes, creando un ambiente de incertidumbre y desconfianza que facilita la manipulación de la opinión pública (Lupiáñez Lupiáñez, 2023).

La manipulación cognitiva ha demostrado ser capaz de alterar no solo la percepción inmediata de la realidad, sino también de configurar patrones de pensamiento y comportamiento a largo plazo (Astorga González, 2020). El impacto de estas narrativas en el dominio cognitivo se amplifica con el uso de tecnologías de la información que permiten una difusión rápida y masiva, lo que hace que los efectos de la desinformación sean más duraderos y difíciles de contrarrestar (Lupiáñez Lupiáñez, 2023).

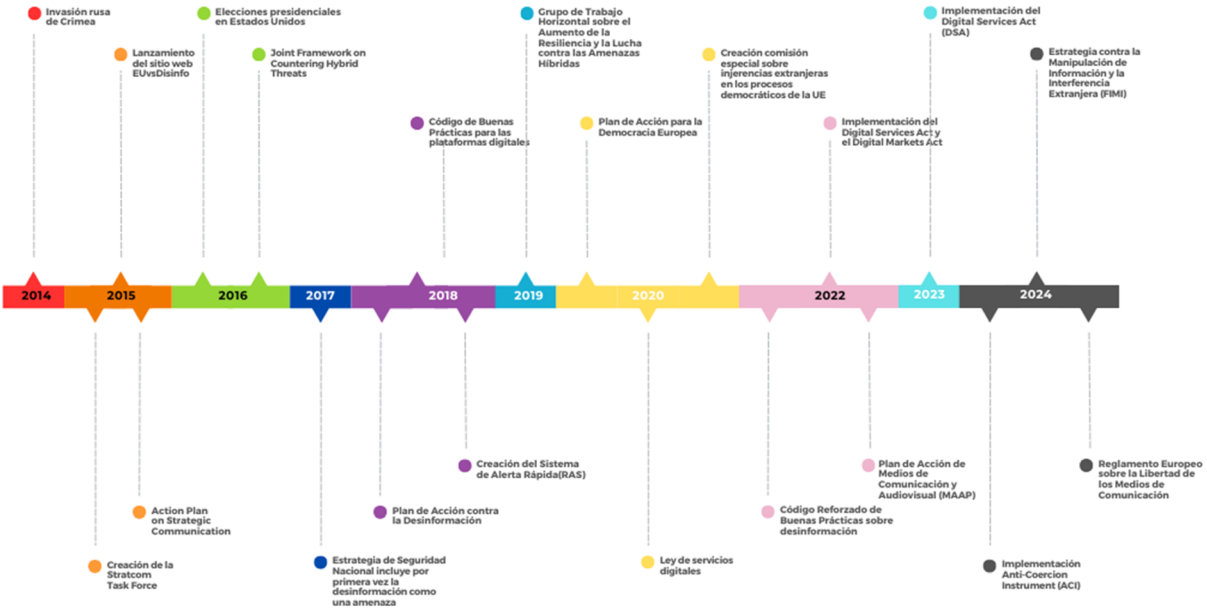
6. EVOLUCIÓN DE LA DESINFORMACIÓN

La UE ha implementado un conjunto de políticas y acciones coordinadas para combatir la desinformación, reconociendo su impacto significativo en la estabilidad democrática y la seguridad de los Estados miembros. La relevancia de esta amenaza se intensificó tras eventos como la invasión rusa de Crimea en 2014 y las elecciones presidenciales en Estados Unidos de 2016, que evidenciaron cómo la desinformación podía ser utilizada como una herramienta eficaz en los conflictos híbridos y en la injerencia electoral (EEAS, 2015). Puede observarse los principales hitos en la Figura 2[15].

[15] Para más información sobre la evolución de las acciones de la UE consultar *España frente a la desinformación: Desafíos híbridos y respuestas convencionales (*Adame Hernández, 2024).

Figura 2

LAS POLÍTICAS DE LA UNIÓN EUROPEA EN LA LUCHA CONTRA LA DESINFORMACIÓN



Fuente: Elaboración propia.

En España la percepción de la desinformación ha evolucionado significativamente en las últimas décadas, a partir de la segunda mitad de la década de 2010, marcada por un creciente reconocimiento de los riesgos asociados a la circulación de información falsa y manipulada, tanto a nivel nacional como internacional (Badillo y Arteaga, 2024).

La polarización política en España, acentuada por el conflicto en Cataluña y la creciente fragmentación del espectro político, ha sido un factor relevante en la percepción de la desinformación (Badillo y Arteaga, 2024). El 60% de los españoles percibían una gran división política en el país, y más del 70% consideraba que la desinformación estaba contribuyendo significativamente a esta división (CIS, 2021).

La confianza de los españoles en los medios de comunicación continúa siendo baja (por debajo del 5 sorbe 10)[16], mientras que la influencia de las redes sociales aumenta [17] (CIS, 2024). El Índice de Confianza en los Medios, elaborado por Eurobarómetro, muestra una desconfianza significativa de los españoles. El 40% de los encuestados en España no confiaba en los medios tradicionales, 12 puntos más que la media europea y el 58% creen que los medios proporcionan información sometida a

[16] En una escala de 1 a 10- sobre la confianza que les merecen los medios de comunicación, la confianza ha pasado del 4,3 en 2021 a la 4,2 en 2022 y al 4,1 en 2023 y 2024. Tendencia más acentuada según disminuye con la edad: el tramo de 25 a 34 años la califica con un 2.88 y el tramo de 18 a 24 con un 3.45 (CIS, 2024).

[1717] El porcentaje de españoles influidos por las redes sociales e internet a la hora de tomar decisiones políticas ha aumentado del 8,6% en 2021, al 9,4% en 2022, el 10,3% en 2023 y el 16,2% en 2024 (CIS, 2024).

presiones políticas o comerciales, 15 puntos más que la media europea (Eurobarómetro, 2024).

La digitalización y la penetración de las redes sociales han jugado un papel crucial en la evolución de la percepción de la desinformación. Según el Digital Economy and Society Index (DESI) de 2024, España ha experimentado un aumento constante en el uso de internet y redes sociales. El DESI indica que, en 2024, el 96.45% de los hogares españoles tenía acceso a internet, el 88.23% de la población tiene habilidades digitales superiores[18] y el 34.4% de las empresas utilizan varias redes sociales (frente al 28.5% de la media europea (DESI, 2020). Este alto nivel de conectividad ha incrementado la exposición de la población a campañas de desinformación. La creciente importancia de las redes sociales como el principal canal de acceso a la información[19], especialmente entre los jóvenes[20], sugiere un alejamiento de los formatos de noticias tradicionales y una preferencia por contenidos visuales y breves (Reuters Institute for the Study of Journalism, 2024).

Finalmente, el contexto global también ha influido en la percepción de la desinformación en España. Por ejemplo, la pandemia de COVID-19, desencadenó una "infodemia", un término acuñado por la Organización Mundial de la Salud para describir la sobreabundancia de información, tanto precisa como inexacta, que dificultó a las personas encontrar fuentes confiables (OMS,2020). Durante la pandemia, la red Latam Chequea verificó más de 1.000 noticias falsas relacionadas con la COVID-19 en España, muchas de las cuales se propagaron ampliamente en redes sociales y aplicaciones de mensajería (Latam Chequea, 2022). Este fenómeno exacerbó la desconfianza pública y desestabilizó aún más el ecosistema informativo, subrayando la necesidad de fortalecer las capacidades nacionales para detectar y contrarrestar la desinformación de manera efectiva (OECD (2024). En medio de una creciente desconfianza en los medios tradicionales, afectando al casi el 70% de la población (Novoa-Jaso, Sierra, Labiano, & Vara-Miguel, 2024). Además, un 37% de los españoles evita activamente las noticias, un comportamiento que parece estar motivado por la saturación de contenido negativo o controversial que domina las narrativas mediáticas actuales (Reuters Institute for the Study of Journalism, 2024).

La respuesta institucional de España a la desinformación ha evolucionado de manera significativa desde 2017, cuando el problema fue reconocido por primera vez en la Estrategia de Seguridad Nacional, hasta la implementación de políticas más robustas y coordinadas en los años siguientes. Sin embargo, esta evolución ha estado marcada tanto

---

[18] Entre las que se incluye enviar/recibir correos electrónicos; Realizar llamadas telefónicas o videollamadas por Internet; Mensajería instantánea; Participar en redes sociales; Expresar opiniones sobre cuestiones cívicas o políticas en sitios web o en redes sociales; Participar en consultas o votaciones en línea para definir cuestiones cívicas o políticas.

[19] WhatsApp ha superado a Facebook como la principal fuente de información en España, con un 36% de los usuarios utilizando WhatsApp para acceder a noticias, frente al 29% que lo hace a través de Facebook. Esta transición resalta un cambio hacia plataformas más privadas y centradas en la mensajería (Reuters Institute for the Study of Journalism, 2024).

[20] TikTok e Instagram están creciendo rápidamente entre los menores de 25 años. TikTok es utilizado por el 30% de este grupo etario para informarse, mientras que Instagram alcanza el 25%, superando a plataformas más tradicionales como YouTube, que se sitúa en un 15% (Reuters Institute for the Study of Journalism, 2024).

por avances notables como por algunas carencias en la integración de enfoques más holísticos que incluyan la gestión de narrativas (Adame Hernández, 2024).[21].

7. MEDIDAS Y HERRAMIENTAS ACTUALES PARA COMBATIR LA DESINFORMACIÓN EN ESPAÑA

El núcleo de la infraestructura española para combatir la desinformación se centra en la Comisión Permanente contra la Desinformación, que coordina la respuesta operativa a campañas de desinformación. Esta comisión actúa bajo la supervisión de la Secretaría de Estado de Comunicación, que lidera la política de comunicación estratégica del Gobierno. En situaciones de crisis, la Célula de Coordinación contra la Desinformación gestiona la respuesta, asegurando que las acciones del Gobierno sean rápidas y efectivas (ORDEN PCM/1030/2020, 2020).

El Foro contra las Campañas de Desinformación en el Ámbito de la Seguridad Nacional, ha sido uno de los pilares principales en la estrategia de España contra la desinformación. En 2023, se presentaron siete documentos que abordan diversas facetas del problema, desde metodologías de verificación y prevención (como el *prebunking* y la teoría de la inoculación[22]) hasta el análisis de la desinformación rusa en el contexto de la guerra en Ucrania. (DSN, 2023b). A finales de 2024, presentaron la segunda edición de trabajos del Foro avanzando en aspectos como el papel que los medios de comunicación y las direcciones de comunicación de instituciones públicas y privadas, FIMI, la relección ente desinformación y discurso del odio e hipótesis de trabajo sobre el ecosistema mediático y de opinión pública español en relación con la desinformación (DSN, 2024b). El Foro canaliza la cooperación público-privada y público-social, articulando un enfoque estratégico y multisectorial. La profundidad de sus análisis, así como los esfuerzos por abordar una realidad compleja, se evidencian con claridad en la evolución de sus respectivas publicaciones.

U otras iniciativas como las campañas de comunicación positiva del Ministerio de Asuntos Exteriores, Unión Europea y Cooperación para combatir la desinformación a través de narrativas verificables[23], el desarrollo de herramientas tecnológicas como ELISA[24] (Estudio Simplificado de Fuentes Abiertas) o el proyecto DANGER (INCIBE. (2024), el Plan de Acción por la Democracia[25] (MPJRC, 2024) o la orden por la que se

[21] Para más información sobre la evolución de las políticas de España contra la desinformación consultar *España frente a la desinformación: Desafíos híbridos y respuestas convencionales (*Adame Hernández, 2024).

[22] El *prebunking* es una técnica preventiva de comunicación que consiste en exponer a las personas a una versión debilitada de la desinformación antes de que la encuentren, con el fin de aumentar su resistencia y capacidad crítica frente a futuros intentos de manipulación. Esta estrategia es similar a la "inoculación" psicológica, que busca generar inmunidad cognitiva contra las narrativas falsas (Maldita.es, 2023; Roozenbeek et al., 2022).

[23] Destacado las campañas “Voto exterior”, “Tu Consulado”, “Viaja Seguro” e información sobre la Ley de Memoria Democrática (DSN, 2024. p. 103).

[24] ELISA monitorea sitios web sospechosos de fomentar campañas de desinformación, permitiendo una detección temprana y una respuesta más ágil por parte de las autoridades (CCN-CERT, 2019). En 2023, aumentó sus capacidades, integrando algoritmos de inteligencia artificial que permiten identificar patrones de desinformación con mayor precisión (DSN, 2024).

[25] Que prevé, entre otros aspectos, la implementación de Reglamento (UE) 2024/1083 del Parlamento Europeo y del Consejo, de 11 de abril de 2024, por el que se establece un marco común para los servicios de medios de comunicación en el mercado interior y se modifica la Directiva 2010/13/UE (Reglamento Europeo sobre la Libertad de los Medios de Comunicación).

establece la elaboración de la Estrategia Nacional contra las Campañas de Desinformación (Orden PJC/248/2025, 2025). Cabe señalar la carencia de estudios, memorias o análisis sobre el impacto de las medidas institucionales contra de desinformación.

7.1. PROCEDIMIENTO DE ACTUACIÓN CONTRA LA DESINFORMACIÓN

El Procedimiento de actuación contra la desinformación regulado por la Orden PCM/1030/2020, tiene como propósito fundamental la creación de un marco coordinado para detectar, analizar y responder a la desinformación en España (ORDEN PCM/1030/2020, 2020), particularmente en situaciones que afecten la seguridad nacional. Este procedimiento fue aprobado por el Consejo de Seguridad Nacional y se inscribe en el contexto de las estrategias europeas para combatir la desinformación, particularmente aquellas establecidas en el Plan de Acción contra la Desinformación de la UE de 2018.

El procedimiento se articula en cuatro ejes fundamentales: Detección, análisis, respuesta y evaluación; y en cuatro niveles de activación. La Secretaría de Estado de Comunicación es la encargada de la coordinación general, actuando en estrecha colaboración con otros ministerios, el Centro de Situación del Consejo de Seguridad Nacional y el Grupo de Trabajo contra la Desinformación. Este grupo interministerial es responsable de asesorar y proponer acciones al Consejo de Seguridad Nacional, asegurando una respuesta integrada y coherente[26].

La implementación del procedimiento provocó controversia pública y llevó a que varias organizaciones presentaran recursos y denuncias ante el Contencioso-Administrativo[27]. También ha sido criticado por su falta de claridad en la definición de competencias y campos de actuación de las diferentes autoridades involucradas (Gómez, 2020; Garrós Font & Santos Silva, 2021) o la falta de recursos especializados (Badillo y Arteaga, 2024).

El Tribunal Supremo estableció unos límites muy claros en los trabajos y alcance del "Procedimiento de Actuación contra la Desinformación" y los organismos que crea al establecer que no crea ni otorga nuevas competencias ni puede afectar derechos fundamentales (Tribunal Supremo, 2021). Restringiendo así el protocolo a un plan de actuación interna limitado a establecer criterios de coordinación. Asimismo, establece una definición jurídica de desinformación[28], algo que no hacia el procedimiento.

---

[26] El Anexo II recoge el funcionamiento y modo de actuación de la comisión permanente contra la desinformación (ORDEN PCM/1030/2020, 2020).

[27] Para más información sobre el Procedimiento de Actuación contra la Desinformación consultar *España frente a la desinformación: Desafíos híbridos y respuestas convencionales (*Adame Hernández, 2024).

[28] Según la sentencia, la desinformación se entiende como "información verificablemente falsa o engañosa que se crea, presenta y divulga con fines lucrativos o para engañar deliberadamente a la población, y que puede causar un perjuicio público" (Tribunal Supremo, 2021). Esta definición se toma del Procedimiento de Actuación contra la Desinformación (ORDEN PCM/1030/2020, 2020) que a su vez la toma de la Comunicación COM (2018) de la Comisión Europea. El Procedimiento de Actuación contra la Desinformación se limitaba en su punto 1. Contexto a reproducir la definición de la Comisión Europea.

8. CONCLUSIONES

A lo largo del artículo, se ha analizado cómo la desinformación se halla inserta en un contexto más amplio de tácticas y estrategias geopolíticas, destacado su papel FIMI. Este contexto más amplio se enriquece con la consideración de cómo los marcos narrativos se emplean estratégicamente para orientar el debate público hacia narrativas específicas que favorecen los intereses de quienes los construyen, minimizando o distorsionando aspectos de la realidad que podrían contradecir estos intereses (Tuñón Navarro, Oleart, & Bouza García, 2019; Astorga González, 2020). Se ha expuesto como la desinformación no actúa como una herramienta aislada, sino que forma parte de un conjunto coordinado de acciones diseñadas para influir en la percepción pública, manipular la narrativa y crear incertidumbre en los procesos políticos y sociales (Hoffman, 2009; McCuen, 2008).

La desinformación ha tenido un impacto crítico en eventos clave durante la última década, impactando tanto la estabilidad institucional como la cohesión social. Los análisis han revelado que las políticas públicas en España, aunque han intentado responder a estas amenazas, han sido insuficientes debido a su carácter fragmentado y predominantemente reactivo (Badillo y Arteaga, 2024). Esto ha puesto a las instituciones españolas en una posición vulnerable frente a campañas de desinformación cada vez más sofisticadas, que han explotado las debilidades en la coordinación interinstitucional y la falta de un enfoque preventivo integral (Bennett & Livingston, 2020).

La respuesta institucional a la desinformación ha sido limitada por la falta de integración entre la ciberseguridad y la defensa cognitiva. El anonimato que brindan las plataformas digitales y la posibilidad de operar a través de intermediarios o "proxies" añade una capa de complejidad que dificulta la identificación de los verdaderos perpetradores de estas campañas (Castro Torres, 2021), lo que fomenta la necesidad de una estrategia más proactiva y prospectiva (Arias Gil, 2019). Aunque se han realizado esfuerzos significativos para mejorar la vigilancia y la respuesta a la desinformación, estos han sido fragmentados y carecen de la coherencia necesaria para enfrentar las amenazas de manera efectiva. Valga como ejemplo la ausencia de una Estrategia Nacional de Lucha Contra las Campañas de Desinformación propuesta desde 2022 (DSN, 2022). Esto se ejemplifica claramente en la activación del Nivel 1 del Procedimiento de Actuación contra la Desinformación. En el nivel más bajo de activación del Procedimiento supone la concurrencia de altos organismos del Estado como la Secretaria de Estado de Comunicación, el DSN, el CNI y la Secretaría de Estado de Transformación Digital e Inteligencia Artificial, entre otros (ORDEN PCM/1030/2020, 2020). Así mismo asigna un rol predominantemente reactivo, lo que refuerza la limitada respuesta y alcance institucional.

Otro ejemplo, la construcción de narrativas y marcos por parte de actores malintencionados ha demostrado ser un desafío formidable, ya que estas tácticas no solo distorsionan la realidad, sino que también debilitan la confianza en las instituciones democráticas (Berger & Luckmann, 2003; Candelas, 2023) un elemento poco abordado en la respuesta institucional española, y donde apuestas como la alfabetización digital o los *fact-checkers* (DSN, 2021) arrojan resultados muy limitados (Pennycook, Bear, Collins, & Rand, 2020; Flynn, Nyhan, & Reifler, 2017). De hecho, las narrativas falsas y altamente engañosas tienden a prevalecer debido a su capacidad para explotar las emociones humanas, como el miedo y la indignación moral, lo que aumenta su impacto y difusión en redes sociales (Pennycook & Rand, 2021).

El análisis de la eficacia de las estrategias propuestas sugiere que un enfoque integral que combine medidas técnicas y cognitivas es fundamental para desarrollar una respuesta eficaz contra la desinformación. Las estrategias actuales, aunque necesarias, no han logrado anticiparse ni responder a las amenazas emergentes debido a su enfoque reactivo (Badillo y Arteaga, 2024) y parcial que no aborda elementos claves del problema como las narrativas. Se hace evidente la necesidad de adoptar una postura más proactiva y prospectiva, que permita a las instituciones no solo responder a las amenazas actuales, sino también anticipar y neutralizar futuras campañas de desinformación (Libicki, 2021).

Una de las iniciativas propuestas por los principales actores es la implementación de tecnologías avanzadas, como la inteligencia artificial y el aprendizaje automático, que pueden desempeñar un papel crucial en la identificación temprana de patrones de desinformación (OTAN, 2021; INCIBE, 2024; DSN, 2024b; Comisión Europea, 2025). Estas tecnologías permiten un análisis en tiempo real de grandes volúmenes de datos, lo que facilita la detección de anomalías que podrían indicar la presencia de campañas coordinadas de desinformación (Rodríguez Lorenzo et al., 2023). Sin embargo, como se ha expuesto a lo largo de este artículo para que estas herramientas sean efectivas, es esencial que se integren en un marco más amplio de defensa institucional, que incluya tanto la ciberseguridad como la defensa cognitiva.

Además de las medidas tecnológicas, la investigación subraya la importancia de fortalecer tanto a la sociedad como a sus instituciones, incrementando su profundidad estratégica y sus capacidades. La lucha contra la desinformación requiere una mayor inversión en recursos económicos, institucionales y humanos (Rodríguez Lorenzo et al., 2023), acorde con la magnitud de la amenaza. Incorporar la lógica de la sociedad híbrida en las propuestas estratégicas y tácticas puede aumentar su efectividad y reducir los costes de inversión en la respuesta (Arias Gil, 2020). Esta lógica permite una mayor adaptación a las amenazas emergentes y una respuesta más eficiente. Es fundamental que España desarrolle capacidades nacionales robustas, especialmente dado que la FIMI no solo involucra a grandes potencias como Rusia y China, sino también a una variedad de actores (Badillo & Arteaga, 2024), para los cuales la respuesta no puede depender exclusivamente de organismos internacionales como la OTAN o la UE.

Es necesario superar el paradigma que se enfoca en el fomento del pensamiento crítico y la alfabetización mediática y avanzar hacia el concepto similar al propuesto por Arias Gil de "ciudadano estratégico" (2020). Este nuevo enfoque implica transformar la lógica de responsabilidad individual, que es pasiva, atomizada, parcial y de desarrollo a medio/largo plazo; en una respuesta social más proactiva, colectiva y coordinada. En lugar de depender únicamente de la formación individual en habilidades críticas, el ciudadano estratégico es un recurso colectivo, proactivo, descentralizado (pero coordinado) que puede actuar rápidamente frente a las amenazas de desinformación. Este cambio de enfoque podría permitir una respuesta más dinámica y eficaz, abordando las amenazas desde el corto plazo y facilitando una mayor adaptación a las tácticas cambiantes de los actores de desinformación.

Una recomendación clave es la necesidad de realizar entrenamientos, simulaciones y maniobras específicas en el ámbito de la desinformación, similares a las que se realizan en otros ámbitos de la seguridad y la defensa. Propuesta ausente en toda la documentación analizada con anterioridad. Estas actividades permitirían a las instituciones estar mejor preparadas para identificar y neutralizar campañas de desinformación antes de que estas

causen un daño significativo. Además, se propone un cambio hacia una postura más proactiva (uso de comunicación estratégica) y prospectiva, que permita identificar los posibles vectores de ataque y tomar medidas preventivas para minimizarlos, neutralizarlos o mitigarlos antes de que se conviertan en amenazas reales. Esto incluye incorporar la lógica asimétrica propia de la sociedad híbrida, donde las respuestas tácticas y estratégicas pueden ser más efectivas y menos costosas (Arias Gil, 2020).

Finalmente, la creación de estructuras más densas y coordinadas en la lucha contra la desinformación se presenta como una medida esencial. Esto incluye la capacitación de mandos intermedios en la administración pública, el sector privado y la sociedad civil, especialmente en áreas relacionadas con la comunicación, la prospectiva y el análisis sociopolítico. Esta formación es crucial para asegurar que todos los sectores de la sociedad estén alineados y preparados para enfrentar las complejas amenazas que plantea la desinformación (DSN, 2022). En este sentido, la disputa por el control de los marcos narrativos se ha convertido en un elemento central en la lucha contra la desinformación, donde no solo se busca combatir las falsedades, sino también establecer marcos alternativos que reconfiguren el debate público (Tuñón Navarro, Oleart, & Bouza García, 2019). De igual modo conocer, eliminar, mitigar o neutralizar las vulnerabilidades culturales, políticas o sociales propias es clave para eliminar vectores de ataque, reducir las vulnerabilidades y aumentar la residencia.

En conclusión, hay una necesidad de un cambio significativo en la forma en que España aborda la desinformación. No basta con implementar medidas técnicas o reactivas; es indispensable desarrollar una estrategia integral que fortalezca los aspectos sociales, cognitivos y tecnológicos, promoviendo una defensa más coordinada, proactiva y adaptativa frente a las amenazas de desinformación en un entorno híbrido global cada vez más dinámico y complejo.

9. REFERENCIAS BIBLIOGRÁFICAS

Adame Hernández, J. F. (2024). España frente a la desinformación: Desafíos híbridos y respuestas convencionales (Trabajo fin de máster, Centro Universitario de la Guardia Civil).

Alastuey Rivas, J., García López, M. I., García Vizcaíno, F., Garrido López, A., Mora Moret, F., Pedrazo Majarrez, J. M., & Pérez-Tejada García, S. (2024). La desinformación como arma de guerra. Documento de Opinión IEEE 26/2024. Instituto Español de Estudios Estratégicos (IEEE). Recuperado de https://www.ieee.es/Galerias/fichero/docs_opinion/2024/DIEEEO26_2024_VVAA_Desinforma (consultado 06/04/2025).

Allcott, H., & Gentzkow, M. (2017). Social media and fake news in the 2016 election. Journal of Economic Perspectives, 31(2), 211-236. https://doi.org/10.1257/jep.31.2.211(consultado 06/04/2025).

Allenby, B., & Garreau, J. (2017, January 3). Weaponized narrative is the new battlespace. Defence One. Recuperado de http://bit.ly/3XyiwB2 (consultado 14/08/2024).

Althusser, L. (1971). Ideología y aparatos ideológicos de Estado. Medellín: La Oveja Negra. Recuperado de https://lobosuelto.com/wp-content/uploads/2018/10/Althusser-L.-Ideolog%C3%ADa-y-aparatos-ideol%C3%B3gicos-de-estado.-Freud-y-Lacan-1970-ed.-Nueva-Visi%C3%B3n-1974.pdf (consultado 14/08/2024).

Arias Gil, E. (2020). Insurgencia low-cost: una amenaza asimétrica emergente. Recuperado de https://canal.uned.es/video/5f6b02325578f274ac7a0632 (consultado 06/04/2025).

Arias Gil, E. (2021). La dimensión emergente de las fake news: La guerra centrada en red y la guerra memética. Recuperado de LA DESINFORMACIÓN COMO SOPORTE DE LAS NARRATIVAS. Jornadas académicas informativas. Memoria. Instituto para el Desarrollo de la Inteligencia en el Ámbito del Terrorismo, Seguridad y Defensa (IDITESDE). https://www.minervainstitute.es/wp-content/uploads/2024/03/IDIT-URJC-1.pdf (consultado 14/08/2024).

Arteaga, Félix (2020). La lucha contra la desinformación: cambio de modelo. Real Instituto Elcano. https://www.realinstitutoelcano.org/comentarios/la-lucha-contra-la-desinformacion-cambio-de-modelo (consultado 06/04/2025).

Astorga González, L. (2020). Manipulación cognitiva en el siglo XXI. Revista del Instituto Español de Estudios Estratégicos, 16, 15-44. Recuperado de https://revista.ieee.es/article/view/2208 (consultado 06/04/2025).

Aznar Fernández-Montesinos, F. (2021). La batalla de las narrativas. Recuperado de LA DESINFORMACIÓN COMO SOPORTE DE LAS NARRATIVAS. Jornadas académicas informativas. Memoria. Instituto para el Desarrollo de la Inteligencia en el Ámbito del Terrorismo, Seguridad y Defensa (IDITESDE).

https://www.minervainstitute.es/wp-content/uploads/2024/03/IDIT-URJC-1.pdf (consultado 14/08/2024).

Badillo, Á. M., & Arteaga, F. (2024). El impacto estratégico de la desinformación en España. Informe Iberifier. Recuperado de https://media.realinstitutoelcano.org/wp-content/uploads/2024/04/informe-iberifier-el-impacto-estratagico-de-la-desinformacion-en-espana.pdf (consultado 06/04/2025).

BBC Mundo (16 de febrero de 2018). El Departamento de Justicia de Estados Unidos acusa a 13 ciudadanos rusos de interferir en las presidenciales de 2016. https://www.bbc.com/mundo/noticias-internacional-43092239 (consultado 04/04/2025).

Bennett, W. L., & Livingston, S. (2020). The disinformation order: Disruptive communication and the decline of democratic institutions. European Journal of Communication. Recuperado de https://iddp.gwu.edu/sites/g/files/zaxdzs5791/files/downloads/The%20Disinformation%20Order%3B%20Livingston.pdf (consultado 14/08/2024).

Berger, P. L., & Luckmann, T. (1966). La construcción social de la realidad. Buenos Aires. Recuperado de https://redmovimientos.mx/wp-content/uploads/2020/07/La-Construcci%C3%B3n-Social-de-la-Realidad-Berger-y-Luckmann.pdf (consultado 06/04/2025).

Burkhardt, J. M. (2017). History of fake news. Library Technology Reports, 53(8), 5-9. https://journals.ala.org/index.php/ltr/article/view/6497/8631 (consultado 06/04/2025).

Buvarp, P. M. H. (2021). The space of influence: Developing a new method to conceptualise foreign information manipulation and interference on social media. The Norwegian Defence Research Establishment (FFI). Recuperado de https://www.ffi.no/en/publications-archive/the-space-of-influence-developing-a-new-method-to-conceptualise-foreign-information-manipulation-and-interference-on-social-media (consultado 02/06/2025).

Calvo Albero, J. L. (18 de diciembre de 2017). Desinformación: viejas ideas en nuevos formatos. Global Strategy. https://global-strategy.org/desinformacion-viejas-ideas-en-nuevos-formatos (consultado 06/04/2025).

Calvo, J. L. (abril, 2023). De la guerra silenciosa a la guerra híbrida. Revista Española de Defensa. https://www.defensa.gob.es/Galerias/gabinete/red/2023/04/p-54-57-red-404-desinformacion.pdf (consultado 06/04/2025).

Candelas, M. (2023). La propaganda en los conflictos geopolíticos: de la guerra psicológica a la guerra más allá de los límites. Documento de Opinión IEEE 02/2023. https://www.ieee.es/Galerias/fichero/docs_opinion/2023/DIEEEO02_2023_MIGCAN_Propaganda.pdf (consultado 06/04/2025).

Caridad-Sebastián, M, Morales-García, A. M., Martínez-Cardama, S, & García López, F (2018). Infomediación y posverdad: el papel de las bibliotecas (Infomediation and post-truth: The role of libraries). https://e-archivo.uc3m.es/bitstream/handle/10016/28096/Infomediacion_EPI_2018.pdf?sequence=1&isAllowed=y (consultado 20/08/2024).

Castro Torres, J. I. (2021). El entorno de la desinformación y la construcción de las narrativas. Recuperado de LA DESINFORMACIÓN COMO SOPORTE DE LAS NARRATIVAS. Jornadas académicas informativas. Memoria. Instituto para el Desarrollo de la Inteligencia en el Ámbito del Terrorismo, Seguridad y Defensa (IDITESDE). https://www.minervainstitute.es/wp-content/uploads/2024/03/IDIT-URJC-1.pdf [URL no disponible] (consultado 14/08/2024).

CCN-CERT. (2019, noviembre 11). ELISA: Nueva herramienta de cibervigilancia del CCN-CERT. Recuperado de https://administracionelectronica.gob.es/pae_Home/pae_Actualidad/pae_Noticias/Anio-2019/Noviembre/Noticia-2019-11-11-ELISA-nueva-herramienta-de-cibervigilancia-del-CCN-CERT.html?idioma=es (consultado 06/04/2025).

Centro de Investigaciones Sociológicas (CIS). (2021). Barómetro CIS de febrero-julio de 2022. Madrid, España. Recuperado de https://www.cis.es/documents/d/cis/es3351marpdf (consultado 14/08/2024).

Centro de Investigaciones Sociológicas (CIS). (2023). Estudio 3424: Percepción social de aspectos científicos de la manipulación genética y biotecnología. Recuperado de https://www.cis.es/es/detalle-ficha-estudio?origen=estudio&codEstudio=3424 (consultado 14/08/2024).

Centro de Investigaciones Sociológicas (CIS). (2024). Estudio 3486: Encuesta sobre Tendencias Sociales (IV). Recuperado de https://www.cis.es/visor?migrado=false&fichero=cru3486_enlace (consultado 01/06/2025).

Chan, R. (2020). The Cambridge Analytica whistleblower explains how the firm used Facebook data to sway elections. https://www.businessinsider.com/cambridge-analytica-whistleblower-christopher-wylie-facebook-data-2019-10 (consultado 06/04/2025).

Chomsky, N. (1992). *Ilusiones necesarias*. Recuperado de https://resistir.info/livros/chomsky_ilusiones_necesarias.pdf (consultado 06/04/2025)

Clausewitz, C. von. (1976). De la guerra. Esfera de los Libros. Recuperado de https://www.esferalibros.com/wp-content/uploads/2022/09/De-la-guerra-primeras.pdf (consultado 14/08/2024).

Colom, G. (2018). Guerras híbridas. Cuando el contexto lo es todo. Revista Ejército. Recuperado de https://www.ugr.es/~gesi/Guerras-hibridas.pdf (consultado 20/08/2024).

Colom, G. (2018b). La doctrina Gerasimov y el pensamiento estratégico ruso contemporáneo. Revista del Ejército. Recuperado de https://www.thiber.org/2019/05/11/la-doctrina-gerasimov-y-el-pensamiento-estrategico-ruso-contemporaneo (consultado 06/04/2025).

Comisión Europea. (2022). The Strengthened Code of Practice on Disinformation. Recuperado de https://ec.europa.eu/newsroom/dae/redirection/document/87585 (consultado 20/08/2024).

Comisión Europea. (2024, 17 de diciembre). La Comisión incoa un procedimiento formal contra TikTok sobre los riesgos electorales en virtud de la Ley de Servicios Digitales Recuperado de https://ec.europa.eu/commission/presscorner/detail/es/ip_24_6487 (consultado 22/03/2025).

Comisión Europea. (2025, 15 de abril). La Comisión invierte 140 millones de euros para desplegar tecnologías digitales clave. Recuperado de https://spain.representation.ec.europa.eu/noticias-eventos/noticias-0/la-comision-invierte-140-millones-de-euros-para-desplegar-tecnologias-digitales-clave-2025-04-15_es#:~:text=La%20Comisi%C3%B3n%20ha%20lanzado%20cuatro,y%20luchar%20contra%20la%20desinformaci%C3%B3n (consultado 22/03/2025).

Dahlgren, P. (2018). *Media, knowledge and trust: The deepening epistemic crisis of democracy*. Javnost - The Public, 25(1–2), 20–27. Recuperado de https://doi.org/10.1080/13183222.2018.1418819 (consultado 06/04/2025).

Davis, G. (2005). The ideology of the visual. In M. Rampley (Ed.), Exploring visual culture: Definitions, concepts, contexts (pp. 163-178). Edinburgh University Press.

DESI dashboard for the Digital Decade. (2024). DESI dashboard for the Digital Decade. Comisión Europea. Recuperado de https://digital-decade-desi.digital-strategy.ec.europa.eu/datasets/desi/charts (consultado 06/04/2025).

DSN. (2021). Estrategia de Seguridad Nacional. Departamento de Seguridad Nacional (2021).

DSN. (2022). Departamento de Seguridad Nacional. (2022). Recuperado de https://www.dsn.gob.es/sites/default/files/documents/LibroDesinfoSN.pdf (consultado 14/08/2024).

DSN. (2023a). Foro contra las Campañas de Desinformación en el ámbito de la Seguridad Nacional - Trabajos 2023. Recuperado de https://www.dsn.gob.es/sites/dsn/files/Foro%20Campa%C3%B1as%20Desinfo%20GT%202023%20Accesible.pdf (consultado 14/08/2024).

DSN. (2023b). Presentación de trabajos 2023: Foro contra campañas de desinformación en el ámbito de la seguridad nacional. Recuperado de https://www.dsn.gob.es/es/actualidad/sala-prensa/presentaci%C3%B3n-trabajos-

2023-foro-contra-campa%C3%B1as-desinformaci%C3%B3n-%C3%A1mbito (consultado 14/08/2024).

DSN. Departamento de Seguridad Nacional. (2024). Informe Anual de Seguridad Nacional 2023. Gobierno de España. Recuperado de https://www.newtral.es/wp-content/uploads/2024/03/IASN2023_0.pdf (consultado 14/08/2024).

DSN. Departamento de Seguridad Nacional. (2024b). Trabajos del Foro contra las Campañas de Desinformación - Iniciativas 2024. Recuperado de https://www.dsn.gob.es/es/publicaciones/otras-publicaciones/trabajos-foro-contra-campanas-desinformacion-iniciativas-2024#:~:text=medios%20de%20comunicaci%C3%B3n.-,Trabajos%20del%20Foro%20contra%20las%20Campa%C3%B1as%20de%20Desinformaci%C3%B3n%20%2D%20Iniciativas%202024,-Accesible (consultado 14/08/2024).

Donoso Rodríguez, D. (2020). *Implicaciones del ámbito cognitivo en las operaciones militares*. *Revista IEEE, 01/2020*. Recuperado de https://emad.defensa.gob.es/Galerias/CCDC/files/IMPLICACIONES_DEL_AMBITO_COGNITIVO_EN_LAS_OPERACIONES_MILITARES.pdf (consultado 01/06/2025).

Dubois, E., & Blank, G. (2018). The echo chamber is overstated: the moderating effect of political interest and diverse media. Information, Communication & Society. Recuperado de https://www.tandfonline.com/doi/full/10.1080/1369118X.2018.1428656#abstract (consultado 06/04/2025).

EEAS (European External Action Service). (2024). 2nd report on FIMI threats - January 2024. Recuperado de https://www.eeas.europa.eu/sites/default/files/documents/2024/EEAS-2nd-Report%20on%20FIMI%20Threats-January-2024_0.pdf (consultado 14/08/2024).

EEAS, European External Action Service. (2015). Tackling disinformation, foreign information manipulation & interference. https://www.eeas.europa.eu/eeas/tackling-disinformation-foreign-information-manipulation-interference_en (consultado 14/08/2024).

ENISA & SEAE. (2022). Foreign Information Manipulation and Interference (FIMI) and Cybersecurity – Threat Landscape. Recuperado de https://www.cde.ual.es/wp-content/uploads/2022/12/EEAS-ENISA-Disinformation_Misinformation.pdf (consultado 14/08/2024).

Eurobarómetro. (2024). EUROBARÓMETRO STANDARD 102 Opinión pública en la Unión Europea. Comisión Europea. Recuperado de https://europa.eu/eurobarometer/surveys/detail/3215 (consultado 14/08/2024).

FIP, Federación Internacional de Periodistas. (2018). ¿Qué son las fake news? Guía para combatir la desinformación en la era de posverdad. Recuperado de

https://www.ifj.org/fileadmin/user_upload/Fake_News_-_FIP_AmLat.pdf (consultado 06/04/2025).

Flores, J. M. (2022). "Las fake news siempre han existido, pero hoy en día se han visto catapultadas por las redes sociales". Recuperado de https://www.ucm.es/otri/noticias-las-fake-news-siempre-han-existido-pero-hoy-en-dia-se-han-visto-catapultadas-por-las-redes-sociales (consultado 20/08/2024).

Flynn, D., Nyhan, B., & Reifler, J. (2017). La naturaleza y los orígenes de las percepciones erróneas: comprender las creencias falsas e infundadas sobre la política. Political Psychology, 38(6), 1053-1077. https://doi.org/10.1111/pops.12394 (consultado 06/04/2025).

Foucault, M. (1972). La arqueología del saber. Siglo XXI Editores. Recuperado de https://monoskop.org/images/b/b2/Foucault_Michel_La_arqueologia_del_saber.pdf

(consultado 14/08/2024).

Garrós Font, I., & Santos Silva, M. F. (2021). La lucha contra la infodemia: Análisis del procedimiento de actuación contra la desinformación. Revista de Comunicación y Salud, 11(2), 75-89. https://doi.org/10.35669/rcys.2021.11(2).75-89

Gelfert, Axel. (2018). Fake News: A Definition. Informal Logic, 38. Recuperado de https://informallogic.ca/index.php/informal_logic/article/view/5068 (consultado 06/04/2025).

Goffman, E. (2006). Frame analysis: Los marcos de la experiencia. Centro de Investigaciones Sociológicas.

Gómez, A. (2020, 19 de noviembre). El nuevo procedimiento de actuación contra la desinformación: La polémica está servida. Blog de Propiedad Intelectual y NNTT Garrigues. Recuperado de https://blogip.garrigues.com/publicidad/el-nuevo-procedimiento-de-actuacion-contra-la-desinformacion-la-polemica-esta-servida (consultado 06/04/2025).

Hafen, R. (2024). El arte operacional chino: La primacía de la dimensión humana. Military Review. Recuperado de https://www.armyupress.army.mil/Portals/7/military-review/Archives/Spanish/Q2-2024/Hafen-SPA-Q2-2024/Hafen-SPA-Q2-2024-UA.pdf (consultado 14/08/2024).

Herman, E. S., & Chomsky, N. (1988). Los guardianes de la libertad. Recuperado de https://www.labiblioteca.mx/llyfrgell/1783.pdf (consultado 06/04/2025).

Hernández-García, L. A. (2022). La zona gris: una aproximación conceptual desde las FAS. Recuperado de https://www.atalayar.com/opinion/luis-hernandez-garcia-ieee/la-zona-gris-una-aproximacion-conceptual-desde-las-fas/20220412121331136376.html (consultado 06/04/2025).

Hoffman, F. (2009). Hybrid warfare and challenges. Small Wars Journal. Recuperado de https://smallwarsjournal.com/documents/jfqhoffman.pdf (consultado 06/04/2025).

INCIBE. (2024). DANGER: Ciberseguridad para la detección, análisis y filtrado de contenidos falsos o maliciosos en entornos de hiperconectividad. Recuperado de https://www.incibe.es/node/521663 (consultado 06/04/2025).

Jamieson, K. H., & Cappella, J. N. (2008). *Echo chamber: Rush Limbaugh and the conservative media establishment*. Oxford University Press.

Jordán, J. (2018). El conflicto internacional en la zona gris: una propuesta teórica desde la perspectiva del realismo ofensivo. Revista Española de Ciencia Política, No. 48. Recuperado de https://www.ugr.es/~jjordan/Conflicto-zona-gris.pdf

(consultado 20/08/2024).

Juurvee, I., & Mattiisen, M. (agosto de 2020). The bronze soldier crisis of 2007: Revisiting an early case of hybrid conflict. International Centre for Defence and Security. Recuperado de https://bit.ly/3iRyeZe (consultado 06/04/2025).

Latam Chequea. (2022). Noticias falsas sobre la COVID-19 verificadas por la red Latam Chequea. Recuperado de https://chequeado.com/investigaciones/como-la-desinformacion-sobre-covid-19-infecto-a-america-latina (consultado 14/08/2024).

Lazer, D. M. J., Baum, M. A., Benkler, Y., Berinsky, A. J., Greenhill, K. M., Menczer, F., ... & Rothschild, D. (2018). The science of fake news: A research agenda. Science, 359(6380), 1094-1096. Recuperado de https://doi.org/10.1126/science.aao2998 (consultado 14/08/2024).

Libicki, M. C. (2021). Cyberspace in Peace and War. Naval Institute Press. Recuperado de https://www.researchgate.net/publication/343399173_Military_Operations_in_Cyberspace (consultado 06/04/2025).

Lupiáñez Lupiáñez, M. (2023). Cómo hacer frente a un ataque cognitivo: Prototipo de detección de la propaganda y manipulación en operaciones psicológicas dirigidas a civiles durante un conflicto. Revista del Instituto Español de Estudios Estratégicos, (22), 61-93. Recuperado de https://revista.ieee.es/article/view/6058 (consultado 14/08/2024).

MAEUEC, Ministerio de Asuntos Exteriores, Unión Europea y Cooperación. (2021). Estrategia de Acción Exterior 2021-2024. Recuperado de https://www.exteriores.gob.es/estrategia2021-2024.pdf (consultado 14/08/2024).

Maggioni, M., & Magri, P. (2018). Twitter and Jihad: The Communication Strategy of ISIS. Journal of Cyberspace Studies, 2(2), 239-241. Recuperado de https://doi.org/10.22059/jcss.2018.66728 (consultado 14/08/2024).

Maldita.es. (2023). ¿Qué es el prebunking? Así actúa esta técnica contra la desinformación antes de que se difunda. Recuperado de https://maldita.es/nosotros/20230323/prebunking-que-es-antes-desmentido (consultado 06/04/2025).

Marchal González, A. N. (2023). La necesidad de un nuevo tipo delictivo: La desinformación como una amenaza para el orden público. Boletín Criminológico, 1(2023), 1-14. Recuperado de https://revistas.uma.es/index.php/boletin-criminologico/article/view/17222/17250 (consultado 06/04/2025).

Martín Renedo, S. (2022). Las Zonas Grises sobre el terreno. ¿El fin de las guerras convencionales? Documento de Opinión IEEE 93/2022. Recuperado de https://www.ieee.es/Galerias/fichero/docs_opinion/2022/DIEEEO93_2022_SAUMAR_Zonas.pdf (consultado 06/04/2025).

Mayoral, J, Parratt, S, & Morata, M. (2019). Desinformación, manipulación y credibilidad periodísticas: una perspectiva histórica. Historia y Comunicación Social, 24(2), 395-409. Recuperado de https://revistas.ucm.es/index.php/HICS/article/view/66267 (consultado 06/04/2025).

McCuen, J. (2008). Hybrid Wars. Military Review, 88(2), 107-113. Recuperado de https://www.armyupress.army.mil/Portals/7/military-review/Archives/English/MilitaryReview_20080430_art017.pdf (consultado 06/04/2025).

McIntyre, L. (2018). Posverdad. Madrid: Cátedra.

MPJRC. Ministerio de la Presidencia, Justicia y Relaciones con las Cortes. (2024). Plan de acción por la democracia. Recuperado de https://www.mpr.gob.es/prencom/notas/Documents/2024/2024-3002_Plan_de_accion.pdf (consultado 06/04/2025).

Newtral. (2022). El Mundial de fútbol de Catar, un escaparate para los bulos y la desinformación. Recuperado de https://www.newtral.es/bulos-mundial-catar/20221203 (consultado 06/04/2025).

Novoa-Jaso, M. F., Sierra, A., Labiano, R., & Vara-Miguel, A. (2024). Digital News Report España 2024. Calidad periodística y pluralidad: Claves para la confianza informativa en la era de la inteligencia artificial (IA). Servicio de Publicaciones de la Universidad de Navarra. Recuperado de https://www.unav.edu/documents/98033082/0/DNR_2024.pdf (consultado 14/08/2024).

OECD (2024), Hechos frente a falsedades: Fortaleciendo la democracia a través de la integridad de la información, OECD. Publishing, Paris. Recuperado de https://doi.org/10.1787/06f8ca41-es (consultado 14/08/2024).

Olmo, J. A. (2019). Desinformación: concepto y perspectivas. Real Instituto Elcano. Recuperado de https://www.realinstitutoelcano.org/analisis/desinformacion-concepto-y-perspectivas (consultado 06/04/2025).

OMS, World Health Organization. (2020). Managing the COVID-19 infodemic: Promoting healthy behaviours and mitigating the harm from misinformation and disinformation. Recuperado de https://www.who.int/news/item/23-09-2020-managing-the-covid-19-infodemic-promoting-healthy-behaviours-and-mitigating-the-harm-from-misinformation-and-disinformation (consultado 14/08/2024).

Orden PCM/1030/2020, de 30 de octubre, por la que se publica el Procedimiento de actuación contra la desinformación aprobado por el Consejo de Seguridad Nacional. (2020). *Boletín Oficial del Estado*. Recuperado de https://www.boe.es/buscar/doc.php?id=BOE-A-2020-13663 (consultado 14/08/2024).

Orden PJC/248/2025, de 13 de marzo, por la que se publica el Acuerdo del Consejo de Seguridad Nacional de 28 de enero de 2025, por el que se aprueba el procedimiento para la elaboración de la Estrategia Nacional contra las Campañas de Desinformación. (2025). Boletín Oficial del Estado. Recuperado de https://www.boe.es/diario_boe/txt.php?id=BOE-A-2025-5151

OTAN. (2021, 12 de agosto). Countering disinformation: improving the Alliance's digital resilience. Recuperado de https://www.nato.int/docu/review/articles/2021/08/12/countering-disinformation-improving-the-alliances-digital-resilience/index.html (consultado 14/08/2024).

OTAN, Headquarters. (2024). Hybrid threats and hybrid warfare: Reference curriculum. Recuperado de https://www.nato.int/nato_static_fl2014/assets/pdf/2024/7/pdf/241007-hybrid-threats-and-hybrid-warfare.pdf (consultado 14/08/2024).

PDC-01. Publicación Doctrinal Conjunta PDC-01 (A) Doctrina para el empleo de las FAS. Estado Mayor de la Defensa, 2018. Recuperado de https://publicaciones.defensa.gob.es/pdc-01-a-doctrina-para-el-empleo-de-las-fas-libros-papel.html (consultado 14/08/2024).

Pennycook, G., & Rand, D. G. (2021). The psychology of fake news. Trends in Cognitive Sciences, 25(5), 388-402. Recuperado de https://www.cell.com/trends/cognitive-sciences/fulltext/S1364-6613(21)00051-6 (consultado 06/04/2025).

Pennycook, G., Bear, A., Collins, E. T., & Rand, D. G. (2020). Fighting misinformation on social media using crowdsourced judgments of news source quality. Proceedings of the National Academy of Sciences, 117(7), 2775-2785. https://www.pnas.org/doi/abs/10.1073/pnas.1806781116 (consultado 02/06/2025).

Posetti, J., & Matthews, A. (2018). A short guide to the history of 'fake news' and disinformation. International Center for Journalists. Recuperado de https://www.icfj.org/sites/default/files/2018-07/A%20Short%20Guide%20to%20History%20of%20Fake%20News%20and%20Disinformation_ICFJ%20Final.pdf (consultado 06/04/2025).

Quiñones de la Iglesia, F. J. (2021). Desinformación y subversión (2.0): las técnicas de la Guerra Fría reaparecen en el dominio informativo del siglo XXI. Documento Marco IEEE 12/2021. Recuperado de https://www.ieee.es/Galerias/fichero/docs_marco/2021/DIEEEM12_2021_FRAQUI_Desinformacion.pdf (consultado 06/04/2025).

Reuters Institute for the Study of Journalism. (2024). Digital News Report 2024. Oxford University. Recuperado de https://reutersinstitute.politics.ox.ac.uk/es/digital-news-report/2024 (consultado 06/04/2025).

Rid, T. (2021). Desinformación y guerra política. Barcelona: Crítica.

Rodrigo Alsina, M. (2005). La construcción de la noticia. Recuperado de https://www.um.es/tic/LIBROS%20FCI-I/La%20produccion%20de%20la%20noticia.pdf (consultado 20/08/2024).

Rodríguez Lorenzo, E, Morales, R, Crescente, D, Cabello, M. I, & Paz, I. (2023). La inteligencia artificial en la guerra híbrida como arma de desinformación. Documento de Opinión IEEE. Recuperado de https://www.ieee.es/Galerias/fichero/docs_opinion/2023/DIEEEO61_2023_EDUROD_Inteligencia.pdf (consultado 06/04/2025).

Roozenbeek, J., van der Linden, S., Goldberg, B., Rathje, S., & Lewandowsky, S. (2022). Psychological inoculation improves resilience against misinformation on social media. *Science Advances, 8*. Recuperado de https://www.science.org/doi/10.1126/sciadv.abo6254 (consultado 06/04/2025).

Sartori, G. (2007). La política. Lógica y métodos en las ciencias sociales. Fondo de Cultura Económica. Recuperado de https://maestriainap.diputados.gob.mx/documentos/materia1/sem1/02.pdf (consultado 06/04/2025).

SEAE. (2023). Tackling disinformation: Foreign Information Manipulation and Interference (FIMI). Recuperado de https://www.eeas.europa.eu/eeas/tackling-disinformation-foreign-information-manipulation-interference_en (consultado 14/08/2024).

Tandoc, E. C., Jr., Lim, Z. W., & Ling, R. (2018). Defining fake news: A typology of scholarly definitions. Digital Journalism, 6(2), 137-153. Recuperado de https://doi.org/10.1080/21670811.2017.1360143 (consultado 06/04/2025).

Terán, E. (2019). Desinformación en la UE: ¿Amenaza híbrida o fenómeno comunicativo? Evolución de la estrategia de la UE desde 2015

https://www.idee.ceu.es/Portals/0/Desinformaci%C3%B3n%20en%20la%20UE..pdf (consultado 06/04/2025).

Torres, C. M. (2021). Fake news: la influencia de la posverdad y la desinformación en la política contemporánea. Comunicación y Sociedad, 18(2), 199-217. Recuperado de https://revistas.javeriana.edu.co/index.php/comunicacionysociedad/article/view/31487 (consultado 14/08/2024).

Torres-Soriano, M. R. (2022). Operaciones de influencia vs. desinformación: diferencias y puntos de conexión. Recuperado de https://www.ieee.es/Galerias/fichero/docs_opinion/2022/DIEEEO64_2022_MANTOR_Operaciones.pdf (consultado 01/06/2025).

Tribunal Supremo. (2021, 18 de octubre). Sentencia STS 1238/2021. Recuperado de https://vlex.es/vid/877507365 (consultado 14/08/2024).

Tuñón Navarro, J., Oleart, Á., & Bouza García, L. (2019). Actores Europeos y Desinformación: la disputa entre el fact-checking, las agendas alternativas y la geopolítica. Revista de Comunicación y Ciudadanía Digital, 8(1), 223-238. Recuperado de https://www.redalyc.org/journal/5894/589466348012 (consultado 06/04/2025).

Walker, R. G. (1998). Spec Fi: The United States Marine Corps and Special Operations. Monterrey, Naval Postgraduate School. Recuperado de https://apps.dtic.mil/sti/pdfs/ADA359694.pdf (consultado 14/08/2024).

Wardle, C., & Derakhshan, H. (2017). Information Disorder: Toward an interdisciplinary framework for research and policy making. Council of Europe. Recuperado de https://rm.coe.int/information-disorder-toward-an-interdisciplinary-framework-for-resear/168076277c (consultado 14/08/2024).

Revista Científica del Centro Universitario de la Guardia Civil
Revista Lógos Guardia Civil

Artículo de Investigación

LA INTELIGENCIA EN EL PUNTO DE MIRA: DE LA TEORÍA CLÁSICA A UN NUEVO ENFOQUE EN LA IMPLEMENTACIÓN EN LA ERA DIGITAL

Paula Castro Castañer
Experta de seguridad en Telefónica S.A
Doctoranda en Ciencias Forenses por la Universidad de Alcalá
Máster en Ciberseguridad y Privacidad por la Universitat Oberta de Catalunya
paula.castroc@edu.uah.es
ORCID: 0009-0008-0315-8387

Recibido 14/02/2025
Aceptado 16/06/2025
Publicado 27/06/2025

Cita recomendada: Castro P. (2025). La inteligencia en el punto de mira: De la teoría clásica a un nuevo enfoque en la implementación en la era digital. *Revista Logos Guardia Civil*, 3(2), p.p. 71-100.

Licencia: Este artículo se publica bajo la licencia Creative Commons Atribución-NoComercial-SinDerivadas 4.0 Internacional (CC BY-NC-ND 4.0)
Depósito Legal: M-3619-2023
NIPO en línea: 126-23-019-8
ISSN en línea: 2952-394X

ORCID: 0009-0008-0315-8387

DEDICATORIA

A mi tutor, Hilario, por confiar en mí y apoyarme en todos mis proyectos.

ORCID: 0009-0008-0315-8387

LA INTELIGENCIA EN EL PUNTO DE MIRA: DE LA TEORÍA CLÁSICA A UN NUEVO ENFOQUE EN LA IMPLEMENTACIÓN EN LA ERA DIGITAL

Sumario: 1. INTRODUCCIÓN. 1.1. NOTA METODOLÓGICA. 2. CONCEPTO Y EVOLUCIÓN DE LA INTELIGENCIA. 2.1. TIPOS DE INTELIGENCIA. 2.2. EVOLUCIÓN DE LOS ENFOQUES Y ESTRATEGIAS DE INTELIGENCIA. 3. EL CICLO DE INTELIGENCIA. 4. PROPUESTA DE ACTUALIZACIÓN DEL CICLO DE INTELIGENCIA EN LA ERA DIGITAL: EL MODELO IDEM. 4.1. EJEMPLO PRÁCTICO DE LA IMPLEMENTACIÓN DEL MODELO IDEM. 5. CONCLUSIONES 6. REFERENCIAS BIBLIOGRÁFICAS.

Resumen: Este artículo aborda la evolución de la inteligencia en el ámbito de la Defensa y Seguridad, desde los enfoques tradicionales hasta su adaptación a la era digital, estableciendo una propuesta que responda a algunas de las limitaciones señaladas en la literatura sobre el ciclo clásico de inteligencia. Para ello se exploran conceptos clave como la definición del concepto de inteligencia, los diferentes tipos de inteligencia e incluso el tradicional ciclo de inteligencia y sus fases. Además, se presenta una revisión de la evolución y de los diferentes enfoques que se han ido adoptando a lo largo de la historia en materia de inteligencia. Por último, se propone un modelo de inteligencia, denominado IDEM, con fases flexibles y que combine el talento del analista humano y el procesamiento automatizado de grandes volúmenes de datos para garantizar una inteligencia proactiva, adaptativa y de calidad ante las complejas amenazas cibernéticas transnacionales.

Abstract: This article addresses the evolution of intelligence in the field of Defence and Security, from traditional approaches to its adaptation in the digital age, proposing an approach that responds to some of the limitations identified in the literature regarding the classical intelligence cycle. Key concepts such as the definition of the concept of intelligence, different types of intelligence, and the traditional intelligence cycle and its phases are explored. Additionally, a review of the evolution and various approaches adopted throughout history in intelligence is presented. Finally, a proposed intelligence model called IDEM is introduced, featuring flexible phases and combining the expertise of human analysts with the automated processing of large volumes of data. This aims to ensure proactive, adaptive, and high-quality intelligence in the face of complex transnational cyber threats.

Palabras clave: Amenazas cibernéticas, ciberinteligencia, ciclo de inteligencia, modelo IDEM, enfoque en red

Keywords: Cyber intelligence, cyber intelligence cycle, cyber threats, IDEM model, network approach

ABREVIATURAS

ABI: *Activity-based Intelligence*, Inteligencia Basada en Actividades

CCN-CERT: Centro Criptológico Nacional - *Computer Emergency Response Team*

CESID: Centro Superior de Información de la Defensa

CIA: *Central Intelligence Agency,* Agencia Central de Inteligencia

CIFAS: Centro de Inteligencia de las Fuerzas Armadas

CNI: Centro Nacional de Inteligencia

COMINT: *Communications Intelligence,* Inteligencia de comunicaciones

COP*: Community Policing* o *Community-oriented policing,* Actividad policial orientada a la comunidad

CTI: *Cyber Threat Intelligence*, Ciberinteligencia de amenazas

CYBINT: *Cyber-Intelligence,* Ciberinteligencia

ELINT: *Electronic intelligence*, Inteligencia electrónica

FISINT: *Foreign instrumentation signals intelligence,* Inteligencia de señales de instrumentación extranjera

GEOINT: *Geospatial Intelligence,* Inteligencia geoespacial

HUMINT: *Human Intelligence*, Inteligencia humana

IDEM: Inteligencia Dinámica Enriquecida y Mejorada

IDS: *Intrusion Detection System*, Sistema de Detección de Intrusiones

ILP*: Intelligence-Led Policin*g, Actividad policial basada en la inteligencia

IMINT: *Imagery Intelligence*, Inteligencia de imágenes

ISR: *Intelligence Surveillance and Reconnnaissance),* Inteligencia, vigilancia y reconocimiento

JISR: *Joint Intelligence Surveillance and Reconnnaissance),* Inteligencia, vigilancia y reconocimiento conjuntos

MASINT: *Measurement and Signature Intelligence*, Inteligencia de medidas y firmas

ML: *Machine Learning,* Aprendizaje Automático

NLP: *Natural Language Processing*, Procesamiento de lenguaje natural

OSCE: *Organization for Security and Co-operation in Europe,* Organización para la Seguridad y la Cooperación en Europa

OSINT: *Open-Source Intelligence,* Inteligencia de fuentes abiertas

SCADA: *Supervisory Control and Data Acquisition,* Control de Supervisión y Adquisición de Datos

SECED: Servicio Central de Documentación

SIEM: *Security Information and Event Management*, Gestión de eventos e información de seguridad

SIGINT: *Signal Intelligence*, Inteligencia de señales

SOCMINT: *Social Media Intelligence*, Inteligencia de redes sociales

TCPED: *Tasking, Collection, Processing, Exploitation, Dissemination*, Planteamiento, recogida, tratamiento, explotación y difusión

TTPs: *Threats, Techniques and Procedures*, Tácticas, técnicas y procedimientos

ORCID: 0009-0008-0315-8387

1. INTRODUCCIÓN

En un mundo en el que la Inteligencia Artificial parece acaparar gran parte de la atención y preocupación pública, ¿en qué lugar queda relegada la inteligencia en todas sus otras vertientes? La omnipresencia de la Inteligencia Artificial en los debates contemporáneos a menudo eclipsa la importancia de otros tipos de inteligencia que son fundamentales para el progreso y desarrollo de la humanidad.

La inteligencia humana, en sus múltiples manifestaciones, sigue siendo un pilar insustituible para la prosperidad de la sociedad, más aún en los contextos complejos y cambiantes de esta Era Digital. Una de esas manifestaciones es la inteligencia competitiva que permite obtener recomendaciones accionables a través del procesamiento de información sobre el entorno externo en busca de oportunidades o desarrollos que podrían impactar la posición competitiva de una empresa o país (Lee, 2023). O la inteligencia prospectiva, que, a partir de información pasada y presente, así como de especulaciones futuras, intenta "dibujar" un mapa cognitivo que permita determinar distintas opciones y reducir el nivel de incertidumbre que acompaña a toda decisión (Montero Gómez, 2006).

Es cierto que el crecimiento exponencial de la digitalización, la exposición y la globalización impulsa el origen y la evolución de nuevas formas de inteligencia en respuesta a las nuevas tecnologías y métodos de recopilación de datos, propiciando el nacimiento de inteligencias como la inteligencia de fuentes abiertas (OSINT) o la inteligencia geoespacial (GEOINT), entre otras. Estas disciplinas aprovechan la ingente cantidad de información disponible para proporcionar una visión comprensiva, integrada y detallada de diversos fenómenos. No obstante, la inteligencia no debe limitarse a la recopilación y análisis de datos, sino que también debe integrar consideraciones éticas y evaluar las posibles consecuencias a largo plazo de las decisiones.

En la actualidad la información y la tecnología son vitales para casi todos los aspectos de la vida, por ello la inteligencia desempeña un papel crucial especialmente en el ámbito de la ciberseguridad, ya que la habilidad para anticipar, identificar y mitigar amenazas es esencial para preservar la integridad, confidencialidad y disponibilidad de los sistemas.

Sin embargo, cabe preguntarse: ¿es esta capacidad una realidad en los organismos gubernamentales y privados actuales? ¿Es la inteligencia efectiva en anticipar y mitigar los riesgos crecientes en el ciberespacio? ¿Está el ciclo de inteligencia actualizado para satisfacer las demandas de la Era Digital? Este trabajo se propone realizar un análisis teórico para abordar estas cuestiones y evaluar la efectividad de la inteligencia en el contexto actual.

1.1. NOTA METODOLÓGICA

Para el desarrollo del presente trabajo se ha llevado a cabo una revisión narrativa de la literatura académica y técnica relacionada con la inteligencia en los ámbitos de la defensa y la seguridad, así como con su adaptación al entorno digital. Esta revisión ha servido como base para contextualizar la evolución del concepto, analizar críticamente el ciclo clásico de inteligencia y fundamentar la propuesta del modelo IDEM.

La búsqueda se realizó en bases de datos académicas como Scopus, Google Scholar y Dialnet, además de fuentes institucionales nacionales e internacionales. Se utilizaron

palabras clave en español e inglés tales como "ciclo de inteligencia", "cyber intelligence", "cyber threat intelligence" o "amenazas cibernéticas". Se priorizaron publicaciones recientes (2000-2024) que ofrecieran enfoques teóricos, modelos metodológicos o análisis críticos del proceso de inteligencia. En ocasiones, debido a la falta de bibliografía en fuentes abiertas se consultaron páginas web con renombre o escritas por técnicos especialistas sobre la materia.

Se excluyeron documentos sin respaldo académico o institucional, así como textos que no abordaban específicamente la dimensión estructural o de los procesos de la inteligencia. La literatura seleccionada fue organizada en torno a cinco ejes temáticos: (1) definición del concepto de inteligencia, (2) clasificación de los tipos de inteligencia, (3) evolución histórica y organizativa de los servicios de inteligencia, (4) revisión crítica del ciclo tradicional y (5) propuestas contemporáneas para su adaptación a la era digital.

Este enfoque metodológico ha permitido detectar vacíos teóricos relevantes y servir de base para la elaboración de un modelo actualizado que integre tanto la dimensión humana como las capacidades tecnológicas de la inteligencia en la actualidad.

2. CONCEPTO Y EVOLUCIÓN DE LA INTELIGENCIA

El término inteligencia es un concepto abstracto y complejo de acotar debido a la multitud de enfoques bajo los que puede ser estudiado. Esta dificultad no solo responde a la diversidad de áreas que lo analizan, sino también a los desafíos dentro de un mismo contexto para establecer una única definición.

En el ámbito de la Defensa y Seguridad la mayoría de los autores vinculan el nacimiento de la inteligencia a la aparición de los Estados y las relaciones interestatales. Sin embargo, no existe consenso respecto a su definición se refiere, debido en gran medida a la diferencia de enfoques que adoptan en la práctica los distintos países (Andric & Terzic, 2023). Esta disparidad dificulta tanto el progreso teórico de su estudio como la comprensión profunda de las diversas dimensiones y factores que inciden en su práctica (Payá-Santos, 2023).

En este contexto, una de las primeras clasificaciones fundamentales, la trinidad, fue establecida por Sherman Kent, definiendo tres realidades para este concepto: inteligencia como organización, como proceso y como resultado (Díaz Fernández, 2013).

- **Inteligencia como organización:** hace referencia a los servicios de inteligencia principalmente bajo el amparo de la administración pública como en el caso del Centro Nacional de Inteligencia (CNI) y el Centro de Inteligencia de las Fuerzas Armadas (CIFAS) en España. Estas instituciones tienen entre sus funciones obtener, evaluar, interpretar y difundir inteligencia para proteger y promover los intereses de España, tanto dentro como fuera del país; prevenir, detectar y neutralizar amenazas contra la constitución, los derechos y libertades, la soberanía, la seguridad del Estado, la estabilidad institucional y el bienestar de la población; promover la cooperación con servicios de inteligencia extranjeros y organismos internacionales; interpretar el tráfico de señales estratégicas; coordinar el uso de medios de cifra; garantizar la seguridad de la información clasificada; además de proteger sus propias instalaciones, información y recursos (Jefatura del Estado, 2002).

- **Inteligencia como proceso**: comprende todas las actividades, generalmente englobadas en el denominado ciclo de inteligencia (tratado con mayor profundidad en apartados posteriores), necesarias para cumplir con las demandas de los líderes y que interpretan un entorno, contexto o problema. Estas actividades se consideran un proceso cíclico continuo y van desde la recopilación de información de diversas fuentes, continuando con su posterior análisis y procesamiento, hasta la difusión de los datos de interés a los usuarios finales (Chainey & Chapman, 2013).
- **Inteligencia como producto:** alude al resultado y/o al conocimiento obtenido, en cualquier formato, tras realizar el ciclo de inteligencia. Este producto debe influenciar en la toma de decisiones y estas deben impactar en el contexto interpretado (Chainey & Chapman, 2013).

Recientemente, también se ha propuesto una cuarta dimensión: la **inteligencia como cultura,** definida por Navarro como "el conjunto de iniciativas y recursos que promueven la conciencia de su necesidad y aportan comprensión cívica sobre su realidad" (Payá-Santos, 2023).

Independientemente de la interpretación adoptada, la inteligencia tiene el objetivo de reducir la incertidumbre intrínseca a la condición humana y a la complejidad del mundo contemporáneo en la toma de decisiones para prevenir y evitar cualquier peligro o amenaza (Jordán, 2015).

Para conseguir este cometido, la inteligencia se nutre de conocimientos teóricos relacionados con la política, la economía, las relaciones internacionales, la seguridad, la sociología, la tecnología, la psicología, etc. De ahí que sea imprescindible presentar equipos de expertos de gran calidad en las diferentes materias para abordar los problemas desde múltiples perspectivas y encontrar soluciones más efectivas y con un enfoque trasversal.

El reciente aspecto multidisciplinar de la inteligencia es consecuencia de la ampliación del concepto de seguridad y la creciente complejidad del contexto social donde cada vez son más comunes las amenazas asimétricas y la ciberguerra.

En contraste, una de las cualidades más antigua de la inteligencia es el carácter secreto de sus actividades e información obtenida. No obstante, el crecimiento del uso de fuentes abiertas (OSINT) está cambiando está perspectiva. Además, la globalización y la expansión del uso de Internet también afectan a los conflictos, los cuales cada vez son más transnacionales y requieren la cooperación internacional de los servicios de inteligencia. Aun así, la protección de las fuentes, especialmente las humanas (HUMINT) sigue siendo un principio fundamental, al igual que la necesidad de preservar la discreción en el manejo de la información para evitar contramedidas, desinformación o vulneración de operaciones sensibles.

En definitiva, se podría establecer que la inteligencia engloba el proceso, el producto y la institución que lleva a cabo las diligencias de recopilación, evaluación y procesamiento de información (Knight, 2024) como instrumento de toma de decisiones, con el fin de identificar, advertir y prevenir riesgos y amenazas, reduciendo la incertidumbre (Francisco & Barrilao, 2019). Para lograrlo, estas tareas deben realizarse

de manera intencionada, oportuna, planificada, "secreta" y organizada (Andric & Terzic, 2023).

2.1. TIPOS DE INTELIGENCIA

Existen diversas clasificaciones de la inteligencia, pero una de las más comunes es según el medio en el que se encuentra la información, estableciendo los siguientes tipos (Kamiński, 2019):

- **SIGINT** (*Signal Intelligence*): se obtiene de las interceptaciones de señales independientemente de cómo estas se transmitan. Hay tres subcategorías: la inteligencia de comunicaciones (COMINT), la inteligencia electrónica (ELINT) y la inteligencia de señales de instrumentación extranjera (FISINT). Resulta especialmente relevante en el monitoreo de amenazas digitales y conflictos híbridos.
- **MASINT** *(Measurement and Signature Intelligence)*: basada en la medida de atributos físicos, como emisiones electromagnéticas, propiedades químicas o características acústicas. Se emplea en operaciones militares avanzadas y detección de armas, con el propósito de caracterizar, localizar e identificar a los objetivos.
- **HUMINT** (*Human Intelligence)*: es el método de recopilación de información más antiguo, proveniente de fuentes humanas, ya sea mediante entrevistas, observación directa, infiltración o colaboración de actores locales. Es fundamental en contextos donde las tecnologías no pueden acceder.
- **GEOINT** *(Geospatial Intelligence)* e **IMINT** *(Imagery Intelligence):* inteligencia geoespacial y de imágenes. La primera combina mapas, datos geográficos e información de sensores remotos, mientras que la segunda se centra en el análisis visual de imágenes satelitales, aéreas o de drones.
- **OSINT** *(Open-Source Intelligence)*: inteligencia derivada de la información de dominio público en formato físico, analógico o digital en los diferentes medios de comunicación, como radio, televisión, periódicos, revistas, Internet, bases de datos comerciales, vídeos, gráficos, dibujos, redes sociales, etc. abiertas o informes públicos. Su volumen, accesibilidad y utilidad han aumentado exponencialmente con Internet (Stewart Bertram, 2015).
- **SOCMINT** *(Social Media Intelligence*): en ocasiones, también se menciona como subcategoría de OSINT, centrada en redes sociales. Se emplea para monitorear tendencias, detectar amenazas emergentes, analizar percepciones y rastrear actores específicos (Mahood, 2015).

Sin embargo, otra tipificación muy común es según su finalidad: estratégica, táctica y operacional (Gruszczak, 2018).

- **La inteligencia estratégica:** se enfoca en identificar riesgos, amenazas y oportunidades para apoyar la definición de objetivos y la toma de decisiones, considerando el entorno, actores relevantes, y posibles evoluciones.
- **La inteligencia táctica**: se centra en la planificación y ejecución de operaciones específicas que permitan alcanzar un objetivo de alcance limitado, derivado de los grandes objetivos de la inteligencia estratégica.

- **La inteligencia operativa**: también conocida como inteligencia operacional en el ámbito militar, tiene como propósito permitir la organización y ejecución de actividades para cumplir una misión específica (Jiménez Villalonga, 2018).

La coexistencia y complementariedad entre estas categorías permite construir una inteligencia integral, adaptada a distintos niveles de decisión.

2.2. EVOLUCIÓN DE LOS ENFOQUES Y ESTRATEGIAS DE INTELIGENCIA

Numerosos autores sostienen que la inteligencia es tan antigua como la historia de la Humanidad, dado que ocultar información confidencial y descubrir la de los adversarios ha sido siempre una herramienta para alcanzar y mantener el poder. Así lo evidencian civilizaciones como la antigua China con la sabiduría milenaria del maestro Sun Tzu (Navarro Bonilla, 2005) o la Grecia clásica con los procedimientos de transmisión de información secreta de Eneas el Táctico (Vela Tejada, 1993).

En sus orígenes, la inteligencia fue una herramienta al servicio del poder político, con un enfoque eminentemente militar: conocer la fuerza, ubicación y capacidades del enemigo para facilitar la toma de decisiones del líder. Sin embargo, a medida que las sociedades se complejizaban, también lo hicieron sus amenazas, lo que llevó a expandir progresivamente la inteligencia hacia aspectos sociales, económicos o políticos. De tal forma que las actividades de inteligencia cobran un papel crucial con el nacimiento de los Estados y las relaciones entre ellos, con la finalidad de defender y proteger los intereses nacionales (Andric & Terzic, 2023).

No obstante, no fue hasta mediados del siglo XX, especialmente tras las dos guerras mundiales y la Guerra Fría que las potencias globales comenzaron a organizar formalmente sus servicios de inteligencia (Estados Unidos con la CIA, Reino Unido con el MI6 e Israel con el Mossad).

España, aunque con menor protagonismo internacional en este ámbito, también presenta el primer intento de establecer un servicio de inteligencia alrededor de esa época. En 1972 se creó el Servicio Central de Documentación (SECED) y en 1977 el Centro Superior de Información de la Defensa (CESID), pero no fue hasta 2002 que se fundó el actual CNI (Centro Nacional de Inteligencia, 2023).

A partir de ese punto, la revolución tecnológica y la explosión del volumen de información disponible marcaron un cambio radical: la inteligencia dejó de ser un ámbito cerrado y centralizado exclusivamente en el Estado para convertirse en una actividad transversal, dinámica y con implicaciones más allá del plano político-militar. Aunque la esencia de la inteligencia se mantiene, los métodos, los tiempos y los objetivos han experimentado transformaciones profundas. El acceso masivo a datos a través de fuentes abiertas, la aceleración de los flujos informativos y la globalización de las amenazas redujeron el ciclo de vida de la información y pusieron en entredicho el papel central que antes ocupaba el secreto (Payá-Santos, 2023).

A este nuevo contexto se le sumaron los atentados del 11-S que marcaron un punto de inflexión evidenciando la necesidad de identificar y prevenir amenazas asimétricas y transnacionales, desdibujando la clásica distinción entre inteligencia interna y externa, y

empujando a las instituciones policiales a adoptar modelos más analíticos, preventivos y colaborativos (Knight, 2024).

Con la progresiva extensión de la inteligencia hacia otros ámbitos estratégicos, como el policial, que históricamente había funcionado con una lógica reactiva, las funciones policiales comenzaron a evolucionar de forma significativa Su enfoque clásico, centrado en la respuesta a delitos ya consumados o en la atención a solicitudes de servicio, fue cuestionado a medida que los cambios sociales y la creciente complejidad del crimen exigían nuevas formas de intervención (Organización para la Seguridad y la Cooperación en Europa, 2017). A partir de entonces, diversas corrientes filosóficas influyeron en la labor policial como (Gkougkoudis et al., 2022):

- ***Community Policing* o *Community-oriented policing* (COP):** prioriza la cooperación entre ciudadanos y las fuerzas y cuerpos del estado, fomentando la confianza y la prevención (Carter & Fox, 2019).
- ***Problem Solving Policing***: orientada a la identificación y análisis de los problemas subyacentes al delito desde una perspectiva más amplia y trasversal buscando soluciones estructurales y sostenibles (Organización para la Seguridad y la Cooperación en Europa, 2017).
- ***Zero Tolerance Policing*:** respuesta estricta incluso ante delitos menores, basada en las ideas desarrolladas por dos criminólogos estadounidenses, James Q. Wilson y George Kelling, que en 1982 publicaron un artículo titulado "Broken Windows" (Ventanas rotas) (Grabosky, 1999).

No obstante, en las últimas décadas debido a la complejidad de las amenazas y riesgos, muchos académicos y profesionales han señalado que el enfoque holístico más acertado para combatir la globalización del crimen es el de *Intelligence-Led Policing* (ILP) traducido como actividad policial basada en la inteligencia. Este enfoque surgió en la década de 1990 en Reino Unido como una estrategia para mejorar la eficiencia fiscal de los servicios policiales, es decir optimizar la asignación de recursos, la productividad operativa y la calidad de los resultados de las actividades policiales. En sus inicios se implementaba principalmente para combatir la delincuencia grave y organizada, pero desde entonces, ha evolucionado globalmente como un modelo proactivo, impulsado por el análisis de datos y enfocado en prevenir, reducir y desarticular todo tipo de crimen. En Estados Unidos fueron los eventos del 11 de septiembre de 2001 los que finalmente impulsaron su adopción, centrando su enfoque en formas más complejas de criminalidad (Summers & Rossmo, 2019).

ILP es una filosofía proactiva para identificar y prevenir problemas criminales usando información bruta y análisis mixto (cuantitativo y cualitativo), pero no es una táctica puntual, sino un marco flexible, adaptable y sostenible basado en datos objetivos (Carter & Fox, 2019). Sin embargo, su implementación enfrenta dificultades en cuanto a la claridad terminológica y la integración de datos, además de la necesidad de garantizar el respeto a los derechos humanos en la gestión de la inteligencia.

Paralelamente, el modelo Activity-Based Intelligence (ABI) ha ampliado las capacidades de análisis, especialmente ante amenazas emergentes. Con antecedentes en la Guerra Fría, su desarrollo ha sido impulsado por la necesidad de gestionar y analizar enormes volúmenes de datos generados por tecnologías modernas, como los drones y las redes sociales, especialmente en el contexto de la lucha contra el terrorismo. Los métodos

tradicionales de análisis han demostrado ser inadecuados en este nuevo entorno, ya que los analistas pasan demasiado tiempo buscando información y vigilando objetivos conocidos, lo que limita su capacidad para descubrir lo desconocido. ABI mejora este proceso al permitir una correlación en tiempo real de datos provenientes de diversas fuentes, superando las limitaciones de los métodos tradicionales de inteligencia, vigilancia y reconocimiento (ISR, concepto que se explicará más adelante) (Atwood, 2015).

Otro enfoque relevante es el modelo 3i propuesto por Ratcliffe en 2006 basado en tres pilares fundamentales: "interpretar", "influenciar" e "impactar" el entorno criminal. Los analistas deben interpretar activamente el entorno, influir en los decisores quienes, a su vez, utilizan esa inteligencia para diseñar estrategias que afecten el entorno criminal (Budhram, 2015). En 2016 añadió una i más, la de intención, como se puede observar en la Figura 1, destacando la necesidad de claridad y comprensión de los objetivos marcados (Organización para la Seguridad y la Cooperación en Europa, 2017).

Figura 1

El modelo 4-i de Ratcliffe: intención, interpretación, influencia e impacto

Nota: Adaptado de *Guía de la OSCE sobre actividad policial basada en la inteligencia* (p. 24), por OSCE, 2017, OSCE

En suma, la inteligencia ha pasado de ser una actividad altamente secreta y centralizada, a un proceso transversal, interdisciplinar, distribuido y con fuerte apoyo tecnológico. Esta evolución justifica la necesidad de nuevos modelos como IDEM, que integren el análisis humano con el procesamiento automatizado para afrontar amenazas modernas, especialmente en el ciberespacio. Además, esta trayectoria permite observar una creciente convergencia entre las lógicas de seguridad, defensa y tecnología, situando a la inteligencia como un componente clave de la soberanía digital y la resiliencia institucional.

3. EL CICLO DE INTELIGENCIA

Aunque frecuentemente se atribuye a Sherman Kent la formulación científica del método de inteligencia, investigaciones posteriores han demostrado que una metodología rigurosa y un conjunto completo de operaciones (lo que más tarde se denominó ciclo de inteligencia) ya estaban delineados, por ejemplo, durante la Guerra Civil Española (Navarro Bonilla, 2004).

El ciclo de inteligencia aglutina todas las actividades que permiten la transformación de información en bruto en inteligencia y como su nombre indica es de naturaleza cíclica. El ciclo de inteligencia clásico tiene cuatro fases, pero en algunos países se añaden fases diferentes o subfases diferenciadas. Por ejemplo, en España el CCN-CERT establece seis fases para el ciclo de inteligencia: dirección y planificación; recolección; transformación; análisis y producción; difusión y, por último, evaluación (Centro Criptológico Nacional, 2015).

- En la primera fase, denominada **dirección y planificación** se establecen el qué y el cómo, es decir, los requisitos del producto de inteligencia que se quiere obtener y las acciones que se deberán llevar a cabo para obtenerlo. Debe quedar claro el tema de estudio, el alcance, los objetivos, el plazo de entrega y el tipo de informe para que el trabajo en el resto de las fases sea eficiente y se obtengan resultados de mayor calidad y en consonancia con las normas jurídicas nacionales e internacionales (Organización para la Seguridad y la Cooperación en Europa, 2017).
- En la siguiente etapa, **recolección,** se recopilan los datos en bruto, por ejemplo, de las fuentes que se han mencionado anteriormente (SIGINT, MASINT, HUMINT, GEOINT, IMINT, OSINT). Este proceso es complejo, ya que los analistas deben establecer el equilibrio exacto entre recolectar todos los datos necesarios y suficientes sin caer en la sobrecarga de información redundante. Para ello deben conocer la existencia, pertinencia, accesibilidad y fiabilidad de las fuentes seleccionadas, así como las limitaciones legales y los requisitos de autorización (Organización para la Seguridad y la Cooperación en Europa, 2017). Además, la validez y la exactitud de la información deberán ser evaluadas antes de proseguir con el resto de los pasos del ciclo de inteligencia.
- En la fase de **transformación** se convierten los datos en bruto recabados en la anterior etapa en conjuntos estructurados como bases de datos, referencias bibliográficas, etc., transformando la información en aquellos formatos necesarios para continuar con el ciclo y obtener inteligencia. Esta etapa implica catalogar, priorizar y referenciar la información recogida.
- La cuarta fase, de **análisis y producción**, está compuesta por las actividades mediante las que se integra, evalúa, analiza y prepara la información transformada de cara a obtener el producto final. Dentro de esta etapa se pueden establecer dos subfases: en la primera se deben integrar los datos obtenidos de diferentes fuentes para establecer hipótesis e identificar un patrón de inteligencia; la segunda implicaría interpretar los datos, es decir, ir más allá de la información obtenida, refutando o respaldando las hipótesis preestablecidas (Organización para la Seguridad y la Cooperación en Europa, 2017). Generalmente en esta fase se obtiene lo que se denomina *actionable intelligence,* producto de inteligencia que satisface los requisitos definidos en la fase de dirección y planificación y, por tanto, las necesidades del consumidor. Este producto a su vez puede ser de muchos tipos, como un análisis de tendencias, una evaluación a largo plazo, una inteligencia actual, estimativa o de avisos, etc. (Centro Criptológico Nacional, 2015).
- En la etapa de **difusión** se entrega el producto final al consumidor que lo ha solicitado y en caso de ser necesario, y jurídicamente admisible, también se compartirá con otros actores interesados.
- La última fase corresponde a la **evaluación** que permite retroalimentar continuamente todas las fases anteriores del ciclo de inteligencia con los

> resultados obtenidos, permitiendo ajustar y refinar tanto las actividades individuales como el ciclo en su conjunto. Esto resulta especialmente útil para satisfacer de manera óptima las necesidades cambiantes de inteligencia.

Sin embargo, muchos expertos cuestionan este modelo tradicional de inteligencia y una de las críticas manifestadas es la excesiva simplificación de este modelo en comparación con la gran complejidad que realmente presenta el proceso de obtención de inteligencia. Robert Clark señala que este término "se ha convertido en un concepto teológico: nadie cuestiona su validez", a pesar de no establecer los pasos precisos a seguir (Phythian et al., 2013).

Además, Arthur Hulnick señala que la noción de que los clientes de inteligencia orientan a los productores al inicio del ciclo es incorrecta, ya que los clientes a menudo esperan ser alertados por el sistema de inteligencia, por lo que el proceso de recopilación mayoritariamente está impulsado por la necesidad de llenar lagunas en los datos y no por las orientaciones políticas (Pothoven et al., 2023).

Por otro lado, no en todos los casos se acude a los órganos de obtención de datos, muchas veces se consultan directamente las bases de datos existentes y alimentadas durante años para preparar un informe. O puede que sí se soliciten nuevos datos en bruto a los equipos que los recolectan, pero no se suele plantear una nueva demanda de inteligencia a nivel de cliente (Jordán, 2011).

En cuanto a la fase de análisis, no se crítica en sí su definición dentro del ciclo de inteligencia, si no que se manifiesta que es la etapa en la que más errores se cometen, no por falta de información, sino más bien por lo contrario, por sobrecarga de datos que inducen a que informaciones relevantes sean ignoradas o inadecuadamente interpretadas por los analistas (Jordán, 2016). Los analistas han de ser conscientes de sus propios procesos mentales y errores potenciales, evitando caer en simplificaciones cognitivas involuntarias y por supuesto en sesgos. Además, en algunos casos, como en situaciones de crisis, llegan los datos directamente en bruto, sin pasar por esta fase.

En referencia a la fase de difusión, en ocasiones tampoco se pasa por ella, ya que no todos los análisis elaborados llegan a los consumidores. Muchos no son leídos por los destinatarios y se guardan directamente en la base interna. Otras muchas veces los clientes ya tienen las decisiones tomadas e ignoran la inteligencia que no las respalda.

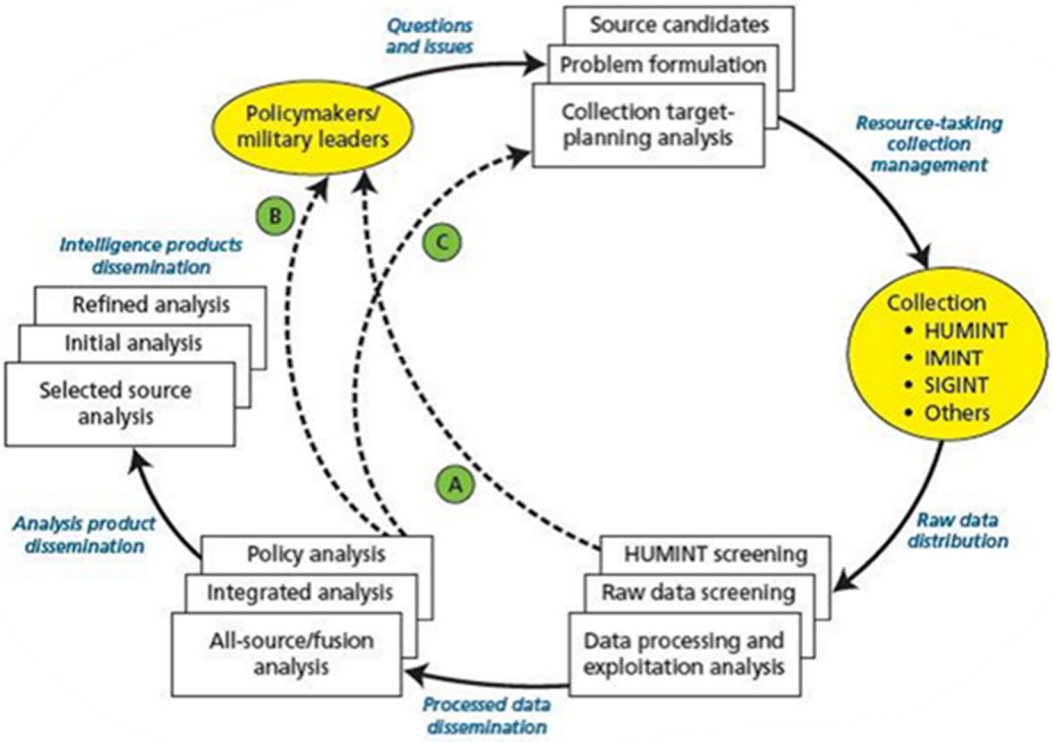
También, en relación con el ciclo de inteligencia de manera general, se critica su definición como una secuencia de fases que finalmente se dispone de manera circular, cuando es un proceso más dinámico, donde todas las fases se retroalimentan entre sí, pudiendo avanzar y retroceder en cualquier dirección dentro del ciclo. Y también se señalan los problemas organizativos, de mando y flujo de información que propician falta de flexibilidad en la acción y comunicación, ralentizando los procesos de toma de decisiones (Organización para la Seguridad y la Cooperación en Europa, 2017).

Referentes como Peter Gill y Mark Phythian argumentan que el concepto del ciclo de inteligencia ha quedado obsoleto debido a los avances tecnológicos, la revolución de la información y los cambios en las amenazas y objetivos. Por lo que proponen reemplazarlo con una "red de inteligencia" que refleja mejor las complejas interacciones entre selección de objetivos, recogida y análisis, y que destaca los factores contextuales

que influyen en el proceso y pueden ser afectados por sus resultados (Pothoven et al., 2023).

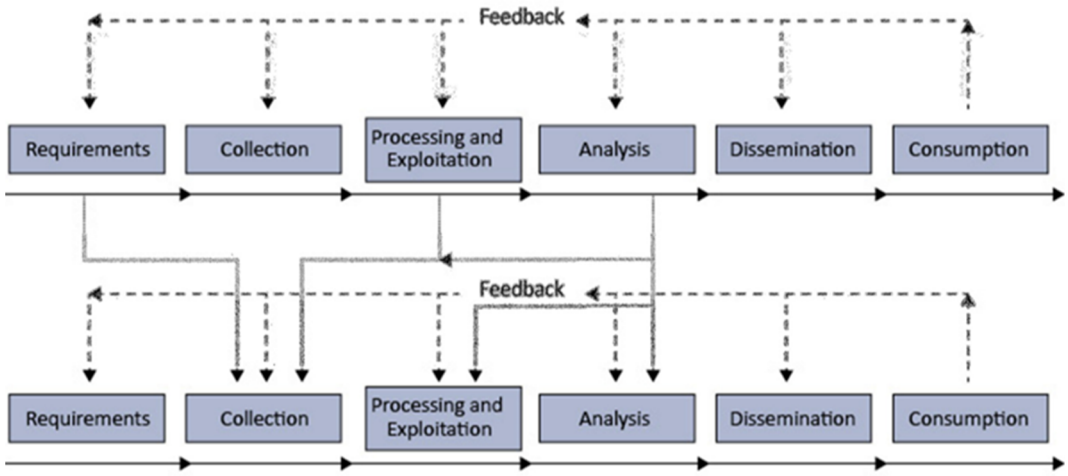
Por otra parte, diversos autores han intentado capturar la complejidad del ciclo de inteligencia en esquemas alternativos al tradicional. Como se puede observar en la Figura 2, Treverton y Gabbard proponen un enfoque más realista que incluye atajos entre fases, mostrando que hay pasos que en ocasiones no se realizan, como por ejemplo que la información no analizada puede llegar directamente a los decisores. Mark Lowenthal presenta un ciclo compuesto por retroalimentaciones constantes, donde nuevas necesidades y ambigüedades reactivan el proceso, haciéndolo más dinámico y con numerosos niveles, como se puede ver en la Figura 3. Y Robert M. Clark introduce el concepto *Target-Centric Intelligence*, un modelo colaborativo y orientado al objetivo, donde todos los participantes construyen juntos una imagen compartida del asunto de interés de la inteligencia, representado en la Figura 4 (Jordán, 2016).

Figura 2
Enfoque de Treverton y Gabbard



Nota: Tomado de *Una revisión del ciclo de Inteligencia* (p. 4) por J. Jordán, 2016, *Análisis GESI (Grupo de Estudios En Seguridad Internacional),* 2.

Figura 3
Proceso multi-estrato Mark Lowenthal



Nota: Tomado de *Una revisión del ciclo de Inteligencia* (p. 5) por J. Jordán, 2016, *Análisis GESI (Grupo de Estudios En Seguridad Internacional),* 2.

Figura 4
Target-Centric Intelligence de Robert M. Clark

Nota: Tomado de *Una revisión del ciclo de Inteligencia* (p. 6) por J. Jordán, 2016, *Análisis GESI (Grupo de Estudios En Seguridad Internacional),* 2.

Por último, también han surgido propuestas como el concepto JISR de la OTAN, (por sus siglas en inglés, Inteligencia, vigilancia y reconocimiento conjuntos en castellano). Este término hace referencia al conjunto integrado de capacidades de inteligencia y operaciones que sincroniza e integra la planificación y ejecución de todas las capacidades de recolección de información con su procesamiento, explotación y difusión. Este concepto surge de la necesidad de mejorar la compartición de información e inteligencia para prevenir crisis, amenazas terroristas, actividades criminales

transnacionales y ciberamenazas (Gruszczak, 2018). La inteligencia, vigilancia y reconocimiento (ISR) siempre han sido actividades esenciales de las operaciones militares, pero se dividían según los niveles de mando (estratégico, operativo y táctico), o según las diversas disciplinas de inteligencia, dependiendo del tipo y complejidad de las fuentes de información involucradas. En el contexto actual esta división limita el uso óptimo de los especialistas de inteligencia, agencias, fuentes y actividades. Por ello, se propone el modelo JISR donde las actividades de inteligencia, vigilancia y reconocimiento funcionan como una sola unidad, integrándose en todos los niveles y dominios (Ministry of Defence, 2023).

No obstante, el modelo JISR presenta el mismo proceso que el ISR, el cual está formado por 5 fases: planteamiento, recogida, tratamiento, explotación y difusión (TCPED por sus siglas en inglés). La principal diferencia con el ciclo de inteligencia tradicional es que este proceso no se plantea de manera lineal ni circular, sino que se ejecutan las diferentes etapas dinámicamente, de forma secuencial, simultánea o independiente, en función del resultado requerido. No obstante, en este modelo, el proceso ISR sí que suele alinearse con la fase de recolección del ciclo de inteligencia, y los resultados de esta recolección se incorporan en la etapa de procesamiento, además de apoyar el ciclo de decisión.

Sin embargo, este enfoque también enfrenta varias limitaciones. Primero, puede haber una falta de recursos suficientes para satisfacer todos los requisitos, especialmente debido a la alta demanda y baja disponibilidad de ciertas capacidades de recolección. También existen problemas técnicos como limitaciones en el poder computacional y el ancho de banda, que afectan la capacidad para procesar y difundir resultados. Los adversarios pueden interferir mediante ataques a las capacidades de ISR, camuflaje, ocultación y desinformación. Además, el acceso a ISR puede estar limitado por barreras físicas, cognitivas, virtuales, legales y políticas (Ministry of Defence, 2023).

Por ello, la inteligencia como proceso en la actualidad debería alejarse de los modelos lineales y cíclicos tradicionales para adoptar estructuras más fluidas y en red, capaces de responder de manera ágil a las amenazas emergentes y aprovechar el vasto volumen de datos disponibles (Jiménez Villalonga, 2018).

4. PROPUESTA DE ACTUALIZACIÓN DEL CICLO DE INTELIGENCIA EN LA ERA DIGITAL: EL MODELO IDEM

El ciclo clásico de inteligencia ha sido durante décadas la columna vertebral de la inteligencia como proceso. En su momento, esta representación secuencial tuvo sentido, ya que facilitaba la estandarización, la formación de analistas y la gestión de las operaciones. Sin embargo, el modelo presenta importantes limitaciones cuando se traslada a contextos actuales marcados por la complejidad, la incertidumbre y el ritmo acelerado de cambio, especialmente en dominios como el ciberespacio.

En este entorno altamente dinámico, la inteligencia ha adquirido una relevancia crítica como instrumento para comprender y anticipar amenazas, particularmente en el ámbito digital. A medida que las organizaciones expanden su presencia en el ciberespacio para maximizar su visibilidad y alcance, también aumentan su superficie de exposición a posibles ataques. Esta transformación obliga a repensar el papel de la inteligencia más

allá de su formulación clásica, adaptándola a las particularidades de un entorno descentralizado, interconectado y en constante evolución.

Sin embargo, esta adaptación no es sencilla. La proliferación de términos y enfoques refleja tanto la juventud del campo como su rápida expansión. En algunos marcos conceptuales, se utiliza el término ciberinteligencia o CYBINT como un subtipo de COMINT (Jiménez Villalonga, 2018), pero también podría considerarse como un tipo de inteligencia superior que abarca y coordina actividades de OSINT, SIGMINT, SOCMINT e incluso HUMINT (Portillo, 2019).

En el contexto europeo es más común hablar de la ciberinteligencia de amenazas (CTI por sus siglas en inglés), que hace referencia a la aplicación sistemática de inteligencia para identificar, analizar y mitigar amenazas que afectan el ciberespacio. Según Gartner (Lee, 2023), la CTI se basa en conocimientos fundamentados en evidencias, que proporcionan contexto, mecanismos, indicadores y consejos prácticos sobre amenazas emergentes o existentes.

Es por eso por lo que la CTI desempeña un papel crucial, ayudando a las organizaciones a desarrollar una estrategia de seguridad proactiva que les permita entender y anticipar las tácticas, técnicas y procedimientos (TTPs, *Threats, Techniques and Procedures)* de los adversarios. Así mismo, facilita la identificación de amenazas desde su origen y la respuesta efectiva a incidentes antes de que puedan causar daños significativos.

No obstante, a la hora de implementar investigaciones o sistemas de trabajo en este ámbito, persiste una ausencia de ciclos metodológicos específicos y ampliamente aceptados para estructurar el proceso de recolección y análisis de ciberinteligencia. En consecuencia, se tiende a recurrir al ciclo de inteligencia tradicional o a alguno de los enfoques alternativos existentes. Pero como se ha señalado, todos ellos presentan limitaciones importantes para su aplicación efectiva en entornos digitales.

El **modelo clásico** es rígido y secuencial; el **modelo propuesto por Treverton y Gabbard** permite cierta flexibilidad, pero carece de retroalimentación clara; el **modelo Target-Centric** plantea un ciclo continuo más cercano al objetivo, aunque sin una estructura realmente flexible entre fases; y el **enfoque multinivel de Lowenthal** introduce dinamismo, pero mantiene una cierta linealidad y las conexiones bidireccionales entre fases no se entienden del todo.

Tabla 1

Tabla comparativa de los diferentes modelos para representan la inteligencia como proceso

	Modelo clásico	Modelo de Treverton y Gabbard	Modelo de Mark Lowenthal	Modelo Target-Centric
Estructura	Lineal o cíclica (fases sucesivas en círculo)	Semilineal (con posibles "atajos")	Multinivel (con capas activas según necesidad)	Cíclica (centrada en el objetivo)
Inicio del proceso	Por requerimiento del consumidor	Similar al clásico, pero admite reiniciar desde fases intermedias	Desde nuevas necesidades que reactiven fases anteriores	Desde el análisis del objetivo (desde análisis anteriores o desde nuevas necesidades e informaciones)
Fases principales	Dirección y planificación, recolección, transformación, análisis y producción, difusión, evaluación	Similares a las del modelo clásico, pero sin orden estricta ni mención a la retroalimentación	Mismas que el clásico, en capas con ciclos internos y *feedback* continuo	Requisitos y *gaps*, recogida, análisis y difusión, se entrelazan en torno al objetivo
Interacción entre fases	Limitada (retroalimentación al final)	Media (lineal con atajos)	Alta (continua y simultánea)	Media (ciclos conectados por el objetivo)
Flexibilidad y adaptabilidad	Baja (modelo rígido y secuencial)	Media (cierta fluidez, pero mantiene fases definidas)	Alta (orientado a reformular continuamente el proceso)	Media: (dinamismo entorno al objetivo)
Difusión de la inteligencia	Al final del proceso	Puede ser omitida o adelantada si el producto lo requiere	Puede producirse en diferentes niveles y momentos, según el ciclo interno activado	Final del proceso, tras la fase de producción
Retroalimentación	Al final del proceso	No aparece referenciada explícitamente	En todas las fases	No aparece referenciada explícitamente

Es por ello que en este trabajo se propone el modelo de inteligencia IDEM (Inteligencia Dinámica Enriquecida y Mejorada) con un enfoque en red, no lineal y altamente adaptativo, en el que las fases del proceso de inteligencia no se suceden de manera secuencial, sino que interactúan de forma dinámica, flexible y continua, permitiendo una retroalimentación constante entre fases y equipos de trabajo.

Mientras que el modelo tradicional comienza con la **dirección y planificación,** donde se establecen los requisitos de inteligencia en función de las necesidades del decisor, el modelo IDEM propone iniciar con una fase de **identificación y priorización de amenazas** en tiempo real. Una de las críticas más reiteradas al ciclo tradicional es su escasa flexibilidad ya que una vez definidos los objetivos, el proceso tiende a seguir una trayectoria fija, lo que resulta ineficaz en el contexto actual, donde las amenazas evolucionan de forma rápida y no siempre están alineadas con las necesidades previamente establecidas. Por ello, el objetivo de esta fase debe ser detectar y priorizar amenazas emergentes de manera proactiva, sin depender exclusivamente de las directrices iniciales de los consumidores, que a menudo no llegan a tiempo o directamente no se formulan. Esta fase se convertiría en un propio proceso dinámico y continuo,

alimentado por la monitorización constante, el reconocimiento en tiempo real de patrones de amenazas emergentes y la capacidad de reorientar rápidamente los esfuerzos de inteligencia conforme surgen nuevas amenazas o cambios en las condiciones (Dahj, 2022).

La siguiente fase, la **recolección**, sigue siendo fundamental en la inteligencia como proceso, ya que sin datos e información no se puede obtener conocimiento accionable. En el modelo clásico, uno de los mayores desafíos ha sido filtrar de manera efectiva grandes volúmenes de datos para evitar tanto la saturación informativa como la pérdida de información crítica. En la Era Digital, esta tarea se ha vuelto aún más compleja debido al aumento exponencial de la cantidad de fuentes y datos disponibles, impulsado por las nuevas tecnologías, la globalización, y la corta vida útil de la información. IDEM aborda esta complejidad mediante el uso de tecnologías avanzadas como el *machine learning* (ML) y la inteligencia artificial, que permiten una recolección continua y exhaustiva automatizada. A pesar de gestionar volúmenes significativamente mayores, estas herramientas hacen posible filtrar, priorizar y enriquecer la información en tiempo real, garantizando así su relevancia y utilidad.

En esta propuesta, no tiene sentido establecer una fase específica para la **transformación** de los datos como se plantea en el modelo clásico. Gracias a tecnologías avanzadas, como el procesamiento de lenguaje natural (NLP por sus siglas en inglés*)* y herramientas de análisis de *big data*, la conversión de datos en bruto en información relevante y contextualizada puede producirse en múltiples etapas del proceso de forma simultánea. Esto permite que los datos sean procesados, estructurados y analizados en paralelo, facilitando una respuesta ágil ante nuevas informaciones o variaciones en el entorno.

Además, la separación entre la **transformación** y el **análisis** puede llevar a una falta de integración y a una pérdida de contexto durante la transición. Por esta razón, IDEM sustituye estas dos fases del modelo clásico por una única etapa de **contextualización y enriquecimiento** que pone el foco en situar los datos en su contexto, interpretar su relevancia y entender la conexión con otros eventos y patrones. De esta manera el análisis puede actualizarse y ajustarse continuamente conforme emergen nuevos datos y surgen nuevas preguntas, desarrollando una capacidad de adaptación continua. Asimismo, es esencial procesar e integrar la información obtenida de múltiples fuentes de datos ya que facilitan una interpretación más profunda y eficiente, especialmente en el contexto actual de amenazas híbridas. A diferencia del enfoque tradicional, y también de los sistemas ISR clásicos, que establece un proceso individual para cada tipo de fuente (OSINT, HUMINT, SIGINT, COMINT, etc.) (Ministry of Defence, 2023), IDEM propone un modelo interconectado y multisensor, más eficaz en la detección y análisis de fenómenos complejos, tal y como sugiere la doctrina de JISR del Departamento de Defensa de EE. UU., abordada en el apartado 2.2

En cambio, en el modelo IDEM sí se mantiene una etapa específica para la **producción** de inteligencia accionable. Mientras que, en el ciclo tradicional, el análisis y producción se centran en generar informes y recomendaciones que ayuden para la toma de decisiones, IDEM aboga por productos no solo reactivos, sino también predictivos, que permitan anticipar eventos y tendencias o evaluar impactos que faciliten el ajuste de las estrategias y decisiones en tiempo real. El énfasis aquí está en la inteligencia como apoyo a decisiones dinámicas, no como producto cerrado.

Paralelamente al desarrollo de todas estas fases, es indispensable la fase de **retroalimentación** definida en el tradicional ciclo de inteligencia, pero reinterpretándola como un proceso trasversal. Para asegurar una mejora continua y un proceso más eficiente, es crucial que se saquen puntos de mejora o debilidades a lo largo de cada una de las fases. Esto permitirá considerar estas observaciones no solo en los pasos siguientes, sino también en investigaciones futuras, en lugar de esperar hasta obtener el producto final de inteligencia, como ocurre en el modelo tradicional.

Por último, en el ciclo tradicional la **difusión** se reserva para el final del proceso, una vez producido el informe de inteligencia. IDEM rompe con esta lógica, planteando una difusión modular y progresiva, , no solo compartiendo inteligencia como tal, sino también aquellas amenazas reconocidas y clasificadas en la fase de identificación y priorización, o los datos recopilados de las diferentes fuentes disponibles o incluso aquellos datos contextualizados y enriquecidos en diferentes formatos. Evidentemente, esta difusión temprana debe gestionarse de forma cuidadosa, garantizando la protección de las fuentes para evitar contramedidas y desinformación por parte de los objetivos y proteger a las fuentes humanas (HUMINT). Sin embargo, el carácter transnacional de los delitos actuales exige la cooperación internacional de los diferentes servicios de inteligencia y, por tanto, la compartición oportuna y no tardía de información entre ellos para obtener unos resultados más eficaces.

Ahora bien, pese a las capacidades técnicas que ofrece la automatización, el papel del analista humano sigue siendo esencial en cada una de las etapas anteriormente descritas. Las herramientas automatizadas operan dentro de unos parámetros y algoritmos definidos por sus programadores, que son los verdaderamente capaces de interpretar la información en un contexto más amplio, considerando factores culturales, políticos y situacionales. Además, los modelos predictivos carecen de la flexibilidad cognitiva para manejar ambigüedades, contradicciones o excepciones y pueden fallar ante entradas erróneas, datos sesgados o situaciones no previstas.

Los analistas, por el contrario, son capaces de adaptarse, innovar y reajustar sus enfoques en respuesta a nuevos paradigmas, mientras que los modelos de inteligencia artificial necesitan una gran cantidad de datos de entrenamiento para poder desarrollar nuevas metodologías de análisis y no son capaces de aplicar enfoques creativos si surgen nuevas problemáticas. Esta capacidad de los humanos, de colaborar entre equipos, discutir interpretaciones, reestructurar estrategias en función del *feedback* recibido es esencial para la implementación exitosa de estrategias de inteligencia (Jordán, 2011).

Tabla 2
Tabla comparativa del modelo clásico y de la propuesta de modelo IDEM

	Modelo clásico	Modelo IDEM (propuesta propia)
Estructura	Lineal o cíclica (fases sucesivas en círculo)	Modular, dinámica y en red (circunferencias concéntricas e interconectadas)
Inicio del proceso	Por requerimiento del consumidor	Proactivo, sin requerimiento previo
Fases principales	Dirección y planificación, recolección, transformación, análisis y producción, difusión, evaluación	Identificación y priorización, recolección, contextualización y enriquecimiento, producción de inteligencia, retroalimentación y difusión
Interacción entre fases	Limitada (retroalimentación al final)	Alta: fases interactivas y bidireccionales
Flexibilidad y adaptabilidad	Baja (modelo rígido y secuencial)	Muy alta (fases simultaneas y reajustables)
Difusión de la inteligencia	Al final del proceso	Transversal y continua desde fases tempranas del proceso
Retroalimentación	Al final del proceso	Constante: en todas las fases
Tecnología aplicada	No contemplada explícitamente	Integración de tecnologías avanzadas (IA, ML, NLP, *big data*)
Participación humana	Central, pero jerárquico	Combinación sinérgica entre analista humano y herramientas automatizadas
Aplicabilidad en entornos digitales	Limitada	Alta (orientado a amenazas cibernéticas y escenarios complejos)

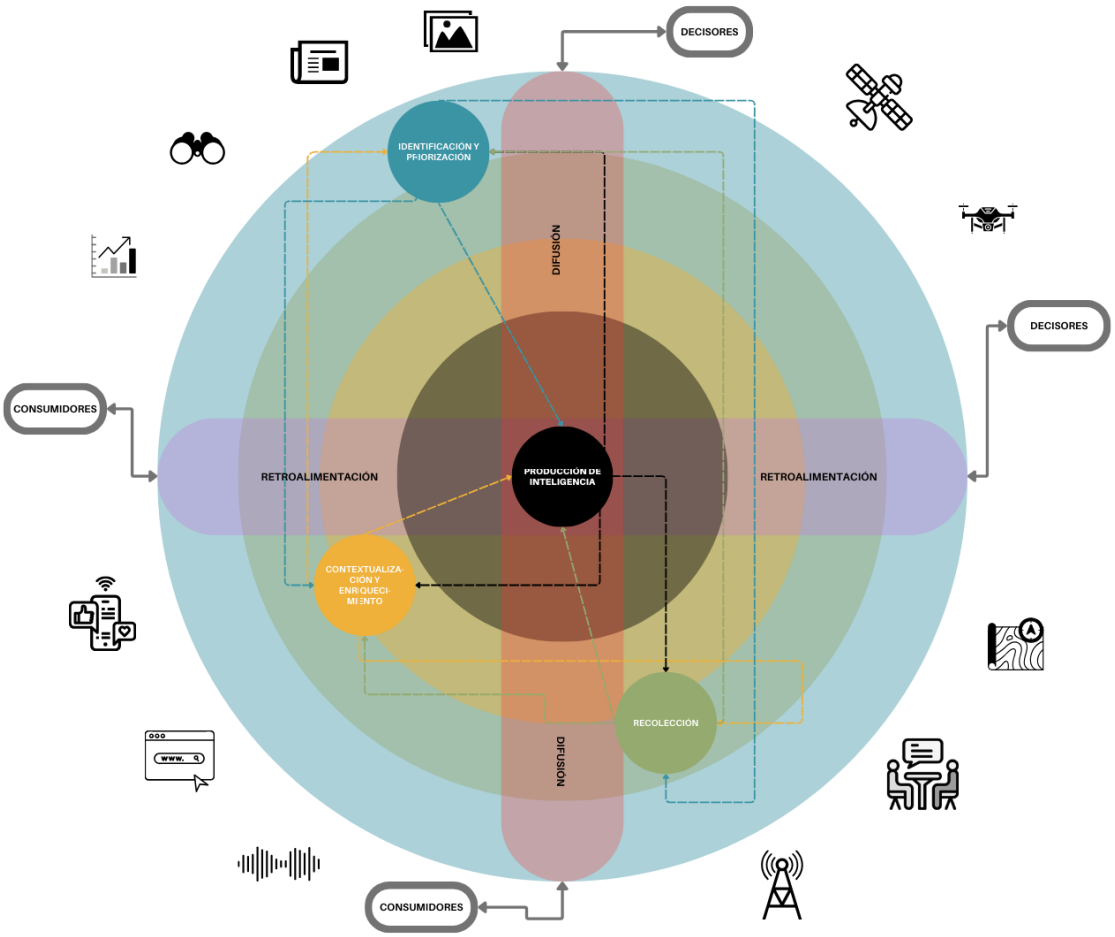
A continuación, se presenta un esquema representativo del modelo IDEM, en el que las diferentes fases se disponen como circunferencias concéntricas. Esta disposición refleja, por un lado, la proximidad creciente al producto final de inteligencia a medida que se avanza hacia el centro, y por otro, y la naturaleza constante de todas las etapas, ya que las fases más internas están contenidas dentro de las exteriores. No obstante, el modelo no establece un recorrido lineal, no es necesario transitar por todas las etapas para poder alcanzar el centro. Este carácter dinámico se representa mediante flechas que indican los posibles flujos de entrada y salida entre las diferentes fases, permitiendo transiciones directas y bidireccionales según las necesidades del contexto.

Perpendicular a estas circunferencias y perpendiculares también entre sí, se integran dos elementos clave representados como rectángulos transversales. El primero representa la fase de retroalimentación, trasversal a todas las fases y oportuna para la mejora continua de todo el ciclo. El segundo simboliza la fase de difusión también colateral a todas las etapas y esencial para obtener productos más completos y resultados más eficaces.

En la parte externa del esquema se sitúan los consumidores y decisores. Su número y relevancia dependerá tanto de las necesidades de inteligencia que se precisen como del impacto esperado de los análisis realizados. Estas figuras se representan mediante flechas bidireccionales, que indican su doble función, establecer el objetivo y los criterios de inteligencia, al mismo tiempo que recibir retroalimentación o productos de inteligencia que les faciliten la toma de decisiones.

Asimismo, se incorporan iconos de diferentes fuentes de información, apoyando así la estrategia de recolectar, contextualizar y enriquecer los datos obtenidos por diferentes fuentes para realizar un proceso de inteligencia más completo, trasversal y eficaz.

Figura 5
Modelo de inteligencia IDEM



Nota: Elaboración propia, Paula Castro Castañer, 2024

La combinación de la adaptabilidad, experiencia, juicio crítico y talento humano con la capacidad de las máquinas para procesar grandes volúmenes de datos crea una sinergia que garantiza una toma de decisiones más efectiva, multidisciplinar, informada y flexible, asegurando una mayor calidad y relevancia de la inteligencia generada.

4.1. EJEMPLO PRÁCTICO DE LA IMPLEMENTACIÓN DEL MODELO IDEM

Un ejemplo práctico que ilustraría la utilidad de aplicar este modelo de inteligencia es en caso de que un proveedor de energía nacional detectará una anomalía en sus sistemas de control SCADA. En esta situación, no existe aún un incidente confirmado ni una solicitud explícita por parte de los decisores (ya que probablemente no tienen conocimiento todavía de esta situación), lo que implica que la activación del proceso de inteligencia se origina de manera proactiva y autónoma, a partir de señales identificadas en el entorno operacional. No obstante, el equipo interno de inteligencia activa el modelo IDEM para anticipar si se trata de una amenaza real o una falsa alarma.

Desde el IDS llega una alerta automática de tráfico anómalo hacia servidores de respaldo, lo cual da inicio a la fase de identificación y priorización. Esta alerta, aunque preliminar, es suficiente para que el equipo interno de inteligencia clasifique la amenaza como prioritaria, considerando el potencial impacto que un compromiso de esta naturaleza podría representar para una infraestructura crítica del país. Como consecuencia, se decide despriorizar temporalmente investigaciones abiertas sobre campañas de hacktivismo y vigilancia geopolítica de bajo impacto, así como otras tareas de monitorización rutinaria en foros y canales oscuros. Esta reorientación permite concentrar esfuerzos humanos y tecnológicos en una única hipótesis de trabajo: una posible intrusión avanzada dirigida.

La recolección se activa simultáneamente desde múltiples fuentes internas (logs, SIEM, registros de autenticación) y externas (feeds de ciberinteligencia, bases de datos de indicadores de compromiso, alertas de entidades colaborados o proveedores de inteligencia). Durante esta etapa, al surgir indicios que sugieren motivaciones económicas detrás del posible ataque, como, por ejemplo, la extracción de datos de mercado en lugar de información operativa, el proceso regresa brevemente a la fase de identificación con el propósito de reformular la hipótesis inicial. Este retorno permite que el análisis se oriente ahora hacia la posibilidad de un caso de espionaje económico industrial en desarrollo, modificando consecuentemente el enfoque del resto de las actividades del proceso de inteligencia.

En la fase de contextualización y enriquecimiento se procede a integrar los datos recopilados con información histórica de incidentes previos y con el análisis de tendencias en el sector energético. Se emplean técnicas de análisis de comportamiento, atribución de TTPs y minería de datos históricos. Estas metodologías facilitan la detección de patrones y coincidencias con campañas anteriormente atribuidas a actores estatales o grupos intermediarios, es decir, entidades que operan como delegados o agentes indirectos de otros actores con intereses geopolíticos o económicos.

La producción de inteligencia se distribuye en distintos formatos adaptados a las necesidades específicas de cada tipo de destinatario. Esto incluiría alertas tácticas dirigidas a los equipos de ciberseguridad responsables de la respuesta inmediata, informes estratégicos orientados a los altos responsables del sistema energético, y recomendaciones preventivas destinadas a otros operadores del sector para fortalecer su postura de defensa.

Es importante destacar que esta producción y difusión de inteligencia se realiza de manera continua y en paralelo con el desarrollo de la investigación, sin esperar a la obtención de una "conclusión definitiva". Este enfoque permite una respuesta temprana y dinámica frente a amenazas emergentes puesto que otros actores relevantes del sector energético al recibir estos productos podrían reportar incidentes similares en sus redes, lo que permitiría reabrir ciclos de análisis y reajustar la priorización de amenazas a escala nacional.

Además de la retroalimentación externa por parte de actores relevantes que permite ajustar hipótesis y prioridades a partir de señales del entorno, también se incorpora una fase de retroalimentación continua interna orientada a la mejora del propio proceso de inteligencia. Por ejemplo, durante la fase de contextualización, el equipo de inteligencia detecta que ciertos indicadores clave de compromiso (IoCs) no fueron

priorizados inicialmente por los sistemas automatizados de alerta. Esta observación se documenta y se canaliza hacia el equipo responsable de ajustar los umbrales de sensibilidad del SIEM, lo que permite refinar los criterios de detección para futuros casos similares. Finalmente, al concluir el ciclo, se realiza una revisión interna del desempeño del modelo IDEM en este caso específico, evaluando métricas como el tiempo de respuesta, la precisión de las hipótesis iniciales y la utilidad de los productos generados. Esta evaluación alimenta una base de conocimiento interna que permite ajustar metodologías, herramientas y flujos de trabajo, asegurando que el modelo evolucione de forma adaptativa y basada en la experiencia acumulada.

Esta dinámica de retroceso, reformulación y acción simultánea que permite el modelo IDEM sería impracticable con el modelo clásico del ciclo de inteligencia, ni en muchos de los modelos propuestos en la literatura revisada, donde los procesos son más rígidos, lineales y dependientes de la iniciativa de los decisores.

5. CONCLUSIONES

La inteligencia, entendida como organización, proceso, producto e incluso cultura, desempeña un papel clave en la gestión de la incertidumbre en entornos volátiles, interconectados y marcados por crecientes amenazas híbridas. Su carácter multidisciplinar y la diversidad de enfoques utilizados por diferentes países y disciplinas dificultan una definición única y una clasificación cerrada de sus tipos, pero también reflejan su riqueza conceptual y la necesidad de cooperación y adaptación constante.

El ciclo clásico de inteligencia, aunque valioso en su momento por aportar estructura y estandarización, presenta limitaciones significativas para enfrentar los retos contemporáneos, especialmente en el ámbito digital. La naturaleza dinámica y descentralizada del ciberespacio, así como el volumen y la velocidad de los datos, requieren modelos más flexibles y adaptativos. El modelo IDEM propuesto en este trabajo responde a esa necesidad mediante una estructura modular, no lineal y en red, donde las fases interactúan de forma simultánea y se retroalimentan constantemente.

Este nuevo enfoque reorganiza las etapas del ciclo tradicional y añade elementos clave como la identificación proactiva de amenazas, la contextualización integrada con el análisis, la difusión temprana y transversal de inteligencia, y la incorporación sistemática de retroalimentación. Además, integra tecnologías avanzadas como la inteligencia artificial o el aprendizaje automático para optimizar la gestión de grandes volúmenes de datos y mejorar la capacidad predictiva.

No obstante, la tecnología por sí sola no basta. El juicio humano, la capacidad crítica, la creatividad analítica y el conocimiento contextual siguen siendo imprescindibles. La sinergia entre analistas y sistemas automatizados garantiza una inteligencia más eficaz, precisa y útil para la toma de decisiones.

En definitiva, la inteligencia del siglo XXI debe ser ágil, multidisciplinar y colaborativa. Solo a través de enfoques híbridos, abiertos al aprendizaje y a la mejora continua, será posible anticipar y mitigar eficazmente las amenazas emergentes. El modelo IDEM es un paso en esa dirección: una propuesta adaptativa y realista para afrontar los desafíos que impone la era digital a los sistemas de inteligencia contemporáneos.

La realidad del contexto actual sigue presentando desafíos y dificultades significativas para anticipar y mitigar de manera efectiva las amenazas contemporáneas, en especial aquellas que se manifiestan en el ciberespacio, puesto que es difícil mantenerse al día y por delante de los ciberdelincuentes. Por ello, es necesario que la comunidad de inteligencia siga investigando y desarrollando estrategias que disminuyan las debilidades actuales, promoviendo la concienciación de la cultura de inteligencia, la difusión de información y la cooperación internacional.

6. REFERENCIAS BIBLIOGRÁFICAS

Andric, J., & Terzic, M. (2023). Intelligence cycle in the fight against terrorism with usage of OSINT data. Journal of Information Systems & Operations Management, 17(1). https://doi.org/10.1080/2158379X.2021.1879572

Atwood, C. P. (2015). Activity-Based Intelligence Revolutionizing Military Intelligence Analysis. Joint Force Quarterly, 77. https://ndupress.ndu.edu/Media/News/Article/581866/activity-based-intelligence-revolutionizing-military-intelligence-analysis/

Budhram, T. (2015). Intelligence-led policing: A proactive approach to combating corruption. South African Crime Quarterly, 52. https://doi.org/10.17159/2413-3108/2015/i52a30

Carter, J. G., & Fox, B. (2019). Community policing and intelligence-led policing: An examination of convergent or discriminant validity. Policing: An International Journal, 42(1), 43–58. https://doi.org/10.1108/PIJPSM-07-2018-0105

Centro Criptológico Nacional. (2015). CCN-STIC-425 Ciclo de Inteligencia y Análisis de Intrusiones.

Centro Nacional de Inteligencia. (2023). Origen de los Servicios de Inteligencia. https://www.cni.es/sobre-el-cni/nuestra-historia

Chainey, S., & Chapman, J. (2013). A problem-oriented approach to the production of strategic intelligence assessments. Policing: An International Journal of Police Strategies & Management, 36(3), 474–490. https://doi.org/10.1108/PIJPSM-02-2012-0012

Dahj, J. N. M. (2022). Mastering Cyber Intelligence. Packt Publishing Ltd.

Díaz Fernández, A. M. (2013). El papel de la inteligencia estratégica en el mundo actual. Cuadernos de Estrategia, 162, 35–66. https://dialnet.unirioja.es/servlet/articulo?codigo=4275959

Francisco, J., & Barrilao, S. (2019). Servicios de Inteligencia, secreto y garantía judicial de los derechos. Teoría y Realidad Constitucional, 309–340.

Gkougkoudis, G., Pissanidis, D., & Demertzis, K. (2022). Intelligence-Led Policing and the New Technologies Adopted by the Hellenic Police. Digital, 2, 143–163. https://doi.org/10.3390/digital2020009

Grabosky, P. N. (1999). Zero tolerance policing. Australian Institute of Criminology, 102(Trends & issues in crime and criminal justice).

Gruszczak, A. (2018). NATO's intelligence adaptation challenge. https://www.globsec.org/what-we-do/publications/natos-intelligence-adaptation-challenge

Jefatura del Estado. (2002). Ley 11/2002, de 6 de mayo, Reguladora del Centro Nacional de Inteligencia.

Jiménez Villalonga, R. (2018, November 26). Tipos de Inteligencia. https://global-strategy.org/tipos-de-inteligencia/

Jordán, J. (2011). Introducción al análisis de inteligencia. 2340-8421, 2, Art. 2. https://www.seguridadinternacional.es/resi/index.php/revista

Jordán, J. (2015). Introducción a la Inteligencia en el ámbito de Seguridad y Defensa. Análisis GESI (Grupo de Estudios En Seguridad Internacional), 26, Art. 26. https://www.seguridadinternacional.es/resi/index.php/revista

Jordán, J. (2016). Una revisión del ciclo de Inteligencia. Análisis GESI (Grupo de Estudios En Seguridad Internacional), 2. https://www.seguridadinternacional.es/resi/index.php/revista

Kamiński, M. A. (2019). Intelligence Sources in the Process of Collection of Information by the U.S. Intelligence Community. Security Dimensions, 32(32), 82–105. https://doi.org/10.5604/01.3001.0014.0988

Knight, T. C. (2024). Five Thousand Candles: Optimizing Information Sharing Policies for Homeland Security A dissertation. American Public University System.

Lee, M. (2023). Cyber Threat Intelligence (1st ed.). John Wiley & Sons, Inc.

Mahood, L. M. E. K. (2015). SOCMINT: following and liking social media intelligence [Canadian Forces College]. https://www.cfc.forces.gc.ca/254-eng.html

Ministry of Defence. (2023). Intelligence, Surveillance and Reconnaissance.

Montero Gómez, A. (2006). Inteligencia Prospectiva de Seguridad (24; Área: Seguridad y Defensa). https://www.realinstitutoelcano.org/publicaciones/

Navarro Bonilla, D. (2004). El Ciclo de Inteligencia y sus límites. Cuadernos Constitucionales de La Cátedra Fadrique Furió Ceriol, 48, 51–66. https://dialnet.unirioja.es/servlet/articulo?codigo=2270935

Navarro Bonilla, D. (2005). Información, espionaje e inteligencia en la monarquía hispánica (Siglos XVI-XVII). Revista de Historia Militar, Extraordinario, 13–40. https://bibliotecavirtual.defensa.gob.es/BVMDefensa/es/catalogo_imagenes/grupo.do?path=309075

Organización para la Seguridad y la Cooperación en Europa. (2017). Guía de la OSCE sobre actividad policial basada en la inteligencia (Departamento de Amenazas Transnacionales Unidad de Asuntos Policiales de carácter estratégico, Ed.; Vol. 13).

Payá-Santos, C. A. (2023). El desempeño de la inteligencia en España en el ámbito público, empresarial y académico. Revista Científica General José María Córdova, 21(44), 1029–1047. https://doi.org/10.21830/19006586.1222

Phythian, M., Warner, M., Gill, P., Richards, J., Davier, P. H. J., Gustafson, K., Ridgen, I., Brantly, A., Sheptycki, J., Strachan-Morris, D., Omand, D., & Hulnick, A. S. (2013). Understanding the Intelligence Cycle (M. Phythian, Ed.).

Portillo, I. (2019). Conociendo que es la Ciberinteligencia y el Cyber Threat Intelligence. https://www.ginseg.com/ciberinteligencia/conociendo-que-es-la-ciberinteligencia-y-el-cyber-threat-intelligence/

Pothoven, S., Rietjens, S., & de Werd, P. (2023). Producer-client paradigms for defense intelligence. Defence Studies, 23(1), 68–85. https://doi.org/10.1080/14702436.2022.2089658

Stewart Bertram. (2015). The Tao of Open Source Intelligence. IT Governance Publishing.

Summers, L., & Rossmo, D. K. (2019). Offender interviews: implications for intelligence-led policing. Policing, 42(1), 31–42. https://doi.org/10.1108/PIJPSM-07-2018-0096

Vela Tejada, J. (1993). Tradición y originalidad en la obra de Eneas El Táctico: La génesis de la historiografía militar. Minerva. Revista de Filología Clásica, 7, 79–92. https://doi.org/https://doi.org/10.24197/mrfc.7.1993

Revista Científica del Centro Universitario de la Guardia Civil
Revista Lógos Guardia Civil

Artículo de Investigación

HACKTIVISMO: DE LA PROTESTA SOCIAL A LA INSTRUMENTALIZACIÓN ESTATAL

Josué Expósito Guisado
Sargento de la Guardia Civil
Doctorando en la Universidad Pablo de Olavide
Máster en Paz, Seguridad y Defensa por el
Instituto Universitario Gutiérrez Mellado (UNED)
jexpgui@gmail.com
ORCID: 0009-0003-4977-3899

Recibido 18/03/2025
Aceptado 05/05/2025
Publicado 27/06/2025

Cita recomendada: Expósito, J. (2025). Hacktivismo: de la protesta social a la instrumentalización estatal. *Revista Logos Guardia Civil*, 3(2), pp. 101-122.

Licencia: Este artículo se publica bajo la licencia Creative Commons Atribución-NoComercial-SinDerivadas 4.0 Internacional (CC BY-NC-ND 4.0)
Depósito Legal: M-3619-2023
NIPO en línea: 126-23-019-8
ISSN en línea: 2952-394X

ORCID: 0009-0003-4977-3899

HACKTIVISMO: DE LA PROTESTA SOCIAL A LA INSTRUMENTALIZACIÓN ESTATAL

Sumario: 1. INTRODUCCIÓN. 2. DE LA PROTESTA SOCIAL A LA CIBERGUERRA. 3.EL NEXO DE UNIÓN ENTRE EL HACKTIVISMO Y LAS APT. 4. EL FUTURO DE LOS GRUPOS HACKTIVISTAS. 5.CONCLUSIONES. 6. REFERENCIAS BIBLIOGRÁFICAS.

Resumen: El hacktivismo ha evolucionado desde una forma inicial de protesta digital hasta convertirse en una herramienta clave en los conflictos geopolíticos contemporáneos. Lo que comenzó como un movimiento descentralizado en defensa de la libertad de expresión y la justicia social, ha sido progresivamente instrumentalizado por los Estados para ejecutar ciberataques, manipular la opinión pública y desplegar operaciones de desinformación. Un fenómeno que se ha visto especialmente acentuado en el marco de la guerra de Ucrania, donde la convergencia entre grupos de Amenaza Persistente Avanzada (APT) y hacktivistas patrióticos ha permitido la ejecución de operaciones cibernéticas coordinadas con los intereses estatales. Paralelamente, la internacionalización del hacktivismo ha llevado a la formación de alianzas entre grupos de distintas regiones, ampliando su impacto más allá del conflicto ruso-ucraniano. El ciberespacio se ha consolidado como un escenario idóneo para la confrontación entre Estados en un entorno controlado. Sin embargo, la creciente sofisticación de los ataques y la selección de objetivos cada vez más estratégicos plantean serios desafíos a la estabilidad internacional y la seguridad de los Estados occidentales.

Abstract: Hacktivism has evolved from an initial form of digital protest into a key tool in contemporary geopolitical conflicts. What began as a decentralized movement advocating for freedom of expression and social justice has been progressively instrumentalized by states to conduct cyberattacks, manipulate public opinion, and deploy disinformation operations. This phenomenon has been particularly pronounced in the context of the war in Ukraine, where the convergence between Advanced Persistent Threat (APT) groups and patriotic hacktivists has enabled the execution of cyber operations aligned with state interests. At the same time, the internationalization of hacktivism has led to the formation of alliances between groups from different regions, expanding its impact beyond the Russia-Ukraine conflict. Cyberspace has become an ideal battleground for controlled confrontation between states. However, the increasing sophistication of attacks and the selection of increasingly strategic targets pose serious challenges to international stability and the security of Western states.

Palabras clave: Hacktivismo, APT, ciberproxies, ciberconflicto, ciberataques.

Keywords: *Hacktivism*, APT, *cyberproxies*, *cyberconflict*, *cyberattacks*.

ABREVIATURAS

APT: Amenaza Persistente Avanzada. (*Advanced Persistent Threat*).

DDoS: Ataque de Denegación de Servicio Distribuido. (*Distributed Denial of Service*).

DOJ: Departamento de Justicia de EE.UU. (*Department of Justice*).

FBI: Buró Federal de Investigaciones. (*Federal Bureau of Investigation*).

GRU: Dirección Principal de Inteligencia de Rusia. (*Glavnoe Razvedyvatel'noe Upravlenie*).

ICS: Sistemas de Control Industrial. (*Industrial Control Systems*).

IRGC: Cuerpo de la Guardia Revolucionaria Islámica de Irán. (*Islamic Revolutionary Guard Corps*).

IT Army of Ukraine: Ejército Informático de Ucrania.

NSA: Agencia de Seguridad Nacional de EE.UU. (*National Security Agency*).

PMC: Empresa Militar Privada. (*Private Military Company*).

PSOA: Actor Ofensivo del Sector Privado. (*Private Sector Offensive Actor*)

SCADA: Control Supervisor y Adquisición de Datos (*Supervisory Control And Data Acquisition*).

Stuxnet: Nombre del *malware* usado en la operación "Olympic Games".

1. INTRODUCCIÓN

La guerra de Ucrania ha supuesto para el mundo occidental enfrentar nuevamente el impacto del realismo político. Antes de la invasión de 2022, la inmensa mayoría de analistas occidentales eran incapaces de vislumbrar en el panorama internacional un conflicto convencional como el que sigue ocurriendo a las puertas de Europa. Cegados por unas doctrinas centradas en el poder blando y siguiendo los paradigmas liberales de la teoría de la paz capitalista o paz comercial, los dirigentes europeos obviaron voluntariamente que, en algunas zonas del mundo, el realismo político sigue imperando.

En un mundo cada vez más digitalizado, donde prácticamente existe una interconexión entre el plano intangible de la informática y el propio espacio físico, no es de extrañar que el actual enemigo de Europa suponga un desafío para la seguridad. A medida que los Estados han aumentado su dependencia de las tecnologías de la información, también han crecido las oportunidades para que actores hostiles (estatales y no estatales) puedan influir en el entorno político y geopolítico mediante el despliegue de acciones en el ciberespacio.

La guerra de Ucrania ha supuesto, no solamente el inicio de una operación de hostigamiento y perturbación cibernética por parte de ciberamenazas vinculadas al Kremlin, sino que también ha provocado un cambio en el panorama hacktivista mundial: lo que hasta hace no tantos años fue el baluarte de la defensa de la libertad de expresión, la privacidad, la justicia social y los derechos humanos, hoy es un instrumento con implicaciones estratégicas y, en muchos casos, vinculado directa o indirectamente con gobiernos y servicios de inteligencia.

El activismo digital con fines ideológicos y de protesta que representaba Anonymous se encuentra en un proceso de evolución hacia un fenómeno conformado por un sinfín de grupos nacionalistas que utilizan de forma reiterada ataques de denegación de servicio distribuido (DDoS) con el objetivo de crear un clima de tensión y de acoso persistente en los enemigos occidentales.

El hacktivismo se ha convertido en una herramienta de doble filo. Por un lado, representa una forma de expresión y lucha por la justicia social, la transparencia y los derechos humanos. Por otro, se ha transformado en un arma utilizada por los Estados para desplegar campañas de desestabilización política y de desinformación.

El empleo de ciberataques con fines geopolíticos ha puesto de manifiesto la delgada línea que existe entre el activismo y el cibercrimen patrocinado por Estados. Este artículo busca analizar la evolución del hacktivismo y su relación con los gobiernos, así como el papel de los grupos de Amenaza Persistente Avanzada (APT) en el uso del ciberespacio con fines políticos y militares[1].

[1] Grupos de ciberatacantes frecuentemente asociados a Estados-nación o grandes organizaciones criminales, altamente sofisticados y persistentes que infiltran redes durante largos períodos para espionaje o sabotaje y que cuentan con recursos abundantes (técnicos, económicos) para atacar objetivos de alto valor (gobiernos, grandes empresas) con premeditación y sigilo.

A través de una revisión de casos concretos, se explorará la colaboración (o instrumentalización) de los hacktivistas por parte de los Estados, las implicaciones de esta práctica y su impacto en la geopolítica actual. Finalmente, se ofrecerá una reflexión sobre el futuro del hacktivismo en un mundo cada vez más interconectado, donde la inteligencia artificial y otras tecnologías emergentes podrían redefinir el papel de estos actores en el ciberespacio.

El hacktivismo ya no es solo un fenómeno marginal de protesta digital, sino un riesgo potencial para la seguridad de los Estados. Comprender su evolución y sus implicaciones resulta fundamental para analizar el futuro de la ciberseguridad española.

2. DE LA PROTESTA SOCIAL A LA CIBERGUERRA

El hacktivismo ha experimentado una notable transformación desde sus orígenes, pasando de ser una forma de protesta social a una herramienta utilizada por los gobiernos para sustentar una agenda política. Si lo pensamos detenidamente, esta transformación traiciona los orígenes y la esencia misma del activismo, por ello, antes de analizar el papel que juega el hacktivismo como herramienta al servicio del Estado, creemos necesario observar el recorrido que ha tenido este fenómeno desde sus orígenes.

En ciertos enfoques contemporáneos, particularmente aquellos orientados a la sistematización terminológica, se tiende a establecer una relación jerárquica entre el ciberactivismo y el hacktivismo, entendiendo al primero como un fenómeno más amplio y que necesariamente abarca al segundo como una manifestación específica o una variante radicalizada. Esta lectura, presente tanto en literatura divulgativa como en algunos marcos analíticos normativos, considera que el ciberactivismo representa la utilización de las tecnologías digitales para la promoción de causas sociales, políticas o culturales mediante campañas de sensibilización, peticiones en línea o protestas virtuales. Por su parte, el hacktivismo se caracterizaría por el uso de herramientas propias del hacking —como los ataques distribuidos de denegación de servicio (DDoS), las filtraciones de datos o la alteración de sitios web— con fines similares, aunque por medios más disruptivos o incluso ilícitos.

Sin embargo, esta interpretación, aunque extendida, resulta problemáticamente reduccionista y no resiste un escrutinio más profundo desde la historia ni desde la teoría crítica de los movimientos digitales. En primer lugar, la suposición de una evolución lineal y progresiva —del ciberactivismo “moderado” al hacktivismo “radical”— ignora las trayectorias históricas diferenciadas de ambos conceptos. El hacktivismo, lejos de ser una derivación tardía del ciberactivismo, emerge de forma simultánea e incluso anterior en determinados contextos, enraizado en la cultura hacker de las décadas de 1980 y 1990, y articulado en torno a principios como la libertad de información, el acceso abierto al conocimiento y la desobediencia civil en el ciberespacio (Jordan & Taylor, 2004; Coleman, 2014).

De hecho, el término "hacktivismo" surge de la combinación etimológica de "hacker" y "activismo", describiendo el uso de habilidades informáticas para promover causas políticas o sociales; y sus raíces se remontan a mediados de la década de 1990, cuando grupos como “*Cult of the Dead Cow*” (La Secta de la Vaca Muerta, en referencia al matadero texano donde el grupo realiza sus reuniones) defendían el acceso universal a

la información en línea como un derecho humano fundamental y la lucha contra los gobiernos opresivos[2].

"Cult of the Dead Cow", considerado uno de los fundadores del hacktivismo moderno, no solo difundía manifiestos críticos sobre el control estatal y corporativo de Internet, sino que también desarrolló herramientas con una clara vocación disruptiva. Entre ellas destaca *Back Orifice* (1998), un software diseñado para exponer las vulnerabilidades del sistema operativo Windows y denunciar las deficiencias en la privacidad de los usuarios[3]. Un año más tarde, en 1999, varios miembros de sus miembros impulsaron el proyecto *Hacktivismo*, una rama explícitamente orientada a la lucha contra la censura digital que dio lugar al desarrollo de herramientas como *Six/Four* o *Peekabooty*, diseñadas para sortear los filtros impuestos por regímenes autoritarios y facilitar el acceso libre a la información.

En el ideario de *Cult of the Dead Cow*, el acceso a la información en línea no solo constituía un derecho fundamental, sino también un campo de disputa política que exigía formas innovadoras de intervención técnica y simbólica. Sin embargo, estas acciones, si bien no eran violentas en términos físicos, implicaban una confrontación directa con las legislaciones restrictivas sobre uso de redes y propiedad intelectual; o, dicho de otra forma, revelaban el carácter ambiguo del hacktivismo.

Por otra parte, conceptualizar el hacktivismo como una simple intensificación táctica del ciberactivismo nos hace perder de vista las divergencias ideológicas y epistemológicas entre ambos. Mientras que el ciberactivismo suele enmarcarse en lógicas de participación ciudadana, incidencia institucional y utilización estratégica de los medios sociales, el hacktivismo opera muchas veces desde el antagonismo directo, la resistencia a las estructuras de poder y el cuestionamiento de los marcos legales vigentes.

Si bien pensar que el hacktivismo constituye una subcategoría del ciberactivismo puede ser útil desde ciertas aproximaciones descriptivas, resulta epistemológicamente insuficiente y empíricamente cuestionable cuando se aborda la genealogía, el marco normativo y las implicaciones ético-políticas de ambas formas de activismo digital. En el presente artículo nos centraremos únicamente en la evolución del hacktivismo, entendido como fenómeno propio, y dejando al margen la formulación de una revisión crítica de esta clasificación.

En los primeros estadios del hacktivismo, el objetivo principal era la realización de ataques contra entidades gubernamentales y corporativas como forma de protesta frente a la censura y las injusticias sociales. Unos mensajes que se fueron recrudeciendo conforme el movimiento antiglobalización de mediados de los noventa emergía en el panorama social (Auty, 2004).

Un hito clave en la consolidación del hacktivismo como herramienta de confrontación política fue la guerra de Kosovo en la década de 1990 (a menudo descrita como la primera guerra librada en línea), donde los contendientes no solo compartían

---

[2] La web de "The Cult of the Dead Cow" a día de hoy aún puede ser consultada en: https://cultdeadcow.com/about.html

[3] Si bien inicialmente fue concebida como una herramienta de auditoría de seguridad, su creación generó cierta controversia y se percibió como una amenaza por la industria tecnológica.

información y testimonios sobre la guerra a través de la red, sino que también difundían propaganda y desinformación. E incluso, surgieron *hackers* que intervinieron activamente en el conflicto desfigurando sitios web gubernamentales y ejecutando ataques de denegación de servicio contra infraestructuras en línea del bando contrario (Denning, 2001).

Académica y socialmente, los movimientos hacktivistas se percibían como la expresión natural de un activismo político preexistente que había sabido encontrar en una nueva herramienta (Internet) la posibilidad de emplear a un tipo de activista con perfil técnico en la expansión de sus mensajes de una forma más mediática (Jordan, 2002).

Sin embargo, el desprecio manifiesto hacia las normas establecidas, los nombres escogidos por los grupos (*The Legion of Doom, Bad Ass Mother Fuckers, Toxic Shock*, etc.) y el contexto de inseguridad social que abrió los atentados del 11-S, hicieron que un fenómeno que inicialmente se percibía positivamente comenzara a suscitar cierta desconfianza. (Torres Soriano, 2018).

La figura del *hacker* comenzó a identificarse con la del criminal, y por extensión, en un contexto geopolítico marcado por la lucha contra el Terror, con la del ciberterrorista. Y las acciones hacktivistas comenzaron a identificarse básicamente como una nueva forma de participación política ilegítima, que empleaba los ciberataques para realizar sabotajes y ciberespionaje (Vegh, 2005).

A nivel académico, la identificación del hacktivismo con lo ilegal o lo criminalizable, frecuente en ciertos discursos, reduce el hacktivismo a una "forma radical de ciberactivismo", y con ello empobrece el análisis y la capacidad explicativa de las ciencias sociales ante la complejidad de las prácticas políticas digitales contemporáneas.

Los inicios de esta década reflejan un hacktivismo marcado por el deseo de sus miembros de transgredir las convenciones sociales por pura diversión. De hecho, las raíces del grupo hacktivista más conocido (Anonymous) se remontan al foro japonés *2chan*, donde la comunidad virtual se dedicaba a compartir todo tipo de contenidos aberrantes relacionados con el anime, el porno y las bromas pesadas (Bartlett, 2015).

Sin embargo, en torno al año 2003, se originan las primeras tensiones internas en una comunidad virtual que había encontrado en el foro *4chan* un espacio ideal para divertirse sin importar las consecuencias. Precisamente, en este foro, algunos usuarios (conocidos como *moralfags*) proponen enfocar sus actividades hacia causas más trascendentales como la lucha contra la censura en Internet, para lavar la imagen del hacktivismo y representar la defensa de la libertad de expresión, la transparencia y otros derechos civiles.

Bajo el lema "*We are Anonymous. We are Legion. We do not forgive. We do not forget. Expect us*." y la máscara de Guy Fawkes, surge un colectivo descentralizado de activistas que combinaban la exfiltración de información y los ataques DDoS para reivindicar la lucha contra la corrupción, la censura y los abusos de poder.

Desde el poder, rápidamente Anonymous fue interpretado como una premonición del riesgo que suponía una nueva generación de actores virtuales motivados, con una estructura sin liderazgo y un funcionamiento basado en la voluntariedad y la

espontaneidad (Olson, 2012). Sin embargo, no fue hasta que el colectivo comenzó a apoyar las acciones de WikiLeaks, cuando el grupo fue percibido como una ciberamenaza de primer nivel.

En poco tiempo, Anonymous pasó de ser un pequeño grupo de *hackers* con inquietudes políticas a convertirse en un movimiento global con miles de seguidores distribuidos por todo el mundo. No obstante, su atractivo no radicaba en una ideología estructurada o en un programa de acción definido. Más allá de su postura antisistema, que los llevó a denunciar la manipulación y el control ejercido por gobiernos y corporaciones, su filosofía carecía de una orientación clara sobre cómo debían organizarse la política, la sociedad o la economía. Esto convirtió a Anonymous en un fenómeno difícil de encasillar, ya que su identidad se basaba más en la acción y la protesta que en una agenda concreta de cambio (Torres Soriano, 2018).

Bajo la máscara de Guy Fawkes se congregaron individuos que ciertamente creían que apoyaban un cambio social positivo, pero también otros: aquellos cuya inspiración era la destrucción nihilista del mundo tal y como lo conocemos y quienes buscaban ocultarse bajo la bandera de Anonymous para obtener un beneficio político o económico.

Del principal legado de Anonymous (el convertir al hacktivismo en una práctica popular que trascendió el ámbito *hacker*) surge una nueva era de hacktivistas que operan en un panorama de fragmentación y complejidad, donde conviven múltiples actores con motivaciones diversas.

Actualmente, si bien grupos como Anonymous continúan operando de forma descentralizada, su impacto ha disminuido en comparación con el auge que llegaron a alcanzar a principios de la década de 2010. En paralelo, han surgido nuevas generaciones de hacktivistas, que, aunque cuentan con un menor nivel de experiencia técnica, lo compensan con el uso de herramientas de automatización y con un dominio del impacto mediático y de la movilización social.

En la actualidad, el hacktivismo es utilizado tanto por colectivos independientes que denuncian injusticias, como por grupos patrocinados por Estados que instrumentalizan estas tácticas con fines geopolíticos. El conflicto entre Rusia y Ucrania ha evidenciado la existencia de una guerra cibernética, en la que hacktivistas pro-ucranianos y pro-rusos llevan a cabo ataques coordinados en beneficio de sus respectivos bandos.

La frontera entre activismo digital legítimo, ciberdelincuencia y operaciones de inteligencia encubiertas es cada vez más difusa. Sin embargo, podríamos considerar que actualmente existen tres tipos de hacktivistas: ciberterroristas, *hackers* cívicos y *hackers* patrióticos (Dahan, 2013; Denning, 2001; Johnson y Robinson, 2014; Sauter, 2013).

El ciberterrorismo comprendería todas aquellas acciones hostiles en el ciberespacio encaminadas a perpetrar actos de violencia contra personas o propiedades, con el objetivo de intimidar o coaccionar a gobiernos o sociedades para alcanzar unos fines políticos, religiosos o ideológicos determinados. Principalmente, sus acciones se concretan en la propagación de virus y *malware*, el vandalismo contra *webs* y la realización de ataques de denegación de servicio (DDoS) o de *botnets* ((Denning, 2001; Jordan y Taylor, 2004; Goode, 2015).

En la categoría de *hackers* cívicos encontraríamos a todos aquellos grupos organizados que realizan acciones contra sistemas informáticos con el objetivo de aportar algún bien a la comunidad, bordeando generalmente la alegalidad. (Hunsinger y Schrock, 2016; Schrock, 2016).

Por último, los *hackers* patrióticos son aquellos individuos o grupos, cuyos esfuerzos se alinean con la ideología nacionalista y se consideran una "milicia cibernética" en pos de la defensa de unos intereses determinados (Dahan, 2013; Green, 2016). Aunque desde el exterior estos *hackers* parezcan no estar directamente patrocinados por ningún Estado, lo cierto es que, actualmente sí que podemos inferir su instrumentalización como parte de un entramado de fuerzas estatales mayor.

El *hackeo* patriótico se originó en China en la década de 1990 como respuesta a los disturbios antichinos en Indonesia, y desde, entonces viene utilizándose como táctica por parte de China, Rusia, Siria y otros Estados como medio para dañar a sus enemigos en el dominio cibernético. No obstante, ninguna de las operaciones anteriores a la guerra de Ucrania había alcanzado la magnitud, el impacto ni unos lazos gubernamentales tan sólidos y prolongados, ni transgredió de manera tan evidente las normas internacionales, como el hacktivismo contemporáneo (Healey & Grinberg, 2022).

3. EL NEXO DE UNIÓN ENTRE EL HACKTIVISMO Y LAS APT

A lo largo de la historia, los Estados han recurrido a actores interpuestos para llevar a cabo sus estrategias de conflicto sin comprometer directamente a sus Fuerzas Armadas. Unidades auxiliares, grupos mercenarios, insurgencias, organizaciones terroristas o empresas militares privadas (PMC) son solamente algunas de las formas que han adoptado terceros actores para actuar como sustitutos en la acción estratégica de los Estados.

Por ello, hoy no resulta sorprendente que, a la luz de una sociedad cada vez más digitalizada, la acción de los Estados haya encontrado en los grupos hacktivistas un nuevo actor para personificar la externalización de la autoría, y en el ciberespacio, el entorno idóneo para proyectar influencia geopolítica.

El concepto de guerra de sustitutos (*surrogate warfare*) ha sido objeto de un debate extenso en la comunidad académica y de seguridad, especialmente por la dificultad que existe para diferenciarlo de la guerra de *proxies*, dada la naturaleza estrechamente entrelazada de ambos conceptos.

En ambos términos, los objetivos del actor principal (el Estado) y el agente apoderado coinciden. Sin embargo, mientras que, en las *proxy warfare* existen dos o más actores relacionados jerárquicamente (el actor principal trabaja por, con y a través del agente apoderado para lograr un objetivo común); en las *surrogate warfare* éstos actores solo se alinean únicamente si el actor principal es capaz de movilizar el apoyo adecuado que exige el agente apoderado (Fox 2019). Dicho de otra forma, los conceptos s*urrogate warfare* y *proxy warfare* difieren en función de la relación existente entre los actores y sus motivaciones.

Dado que los grupos hacktivistas apenas tienen independencia para ejercer resistencia al control del Estado que les patrocina (o al menos, que los influencia o tolera), en nuestro caso de estudio hablaremos en términos de actores *proxies*.

Más concretamente, para referirnos a ellos utilizaremos la definición de Rondeaux y Sterman (2019) de "actores *proxies*", quienes los definen como "*sujetos ajenos a la estructura de seguridad de los Estados involucrados en un conflicto que actúan bajo patrocinio directo o indirecto de un actor convencional (un Estado)*"; y en la definición de Maurer (2018) de *ciberproxies*, como "*intermediarios que llevan a cabo acciones ofensivas en el ciberespacio en beneficio de un actor principal*".

Históricamente, los *ciberproxies* se han personificado a través de distintas entidades vinculadas al mundo de la ciberdelincuencia y el ciberespionaje. No obstante, el término engloba un gran número de entidades organizadas que, de forma directa o indirecta, suponen un factor de riesgo para empresas y Estados. De hecho, la lista de actores es realmente amplia: grupos criminales, empresas privadas de ciberarmas (actores ofensivos del sector privado, en inglés *Private Sector Offensive Actor*, PSOA), grupos terroristas, insurgentes, hacktivistas, actores estales o APT son solamente algunos de ellos.

Las razones detrás de su utilización son variadas: (1) la utilización de actores *proxies* por parte de los gobiernos reduce el riesgo de escalada en los conflictos, dado que la dificultad de atribuir la responsabilidad de un ciberataque es compleja; (2) existe una posibilidad de negación plausible que desvía la responsabilidad de un ataque hacia un actor fuera de control gubernamental; (3) favorece a los Estados alargar la situación de tensión en los conflictos, desgastando a su adversario a un nivel social, político y económico; (4) permite a los Estados actuar al margen de las regulaciones internas y de la crítica de sectores gubernamentales contrarios –o, incluso, de la propia opinión pública en las democracias; (5) aporta a los Estados rapidez y flexibilidad en la respuesta a las acciones ofensivas de sus adversarios, al no exigir evidencias técnicas ni legitimación pública; (6) ofrece a los Estados una herramienta más de disuasión; (7) permite a los Estados eludir la aplicación del derecho internacional; (8) facilita la utilización de personal experto sin necesidad de ofrecer una contratación legal; (9) posibilita participar en conflictos internacionales que en otras circunstancias resultarían económica y políticamente inabarcables (Torres Soriano, 2017; Expósito Guisado, 2024; Marín Gutiérrez, 2023).

No obstante, la consecución de estos beneficios no está exenta de problemáticas. De hecho, el principal atractivo de recurrir a un *proxy* (que no es otro que obtener una negación plausible de una agresión), resulta también su principal debilidad, pues el anonimato y la clandestinidad diluyen la capacidad coactiva y disuasiva del Estado patrocinador –al fin y al cabo, no podemos obviar las teorías Clausewitz que sugieren que para que un Estado modifique su conducta en base a la voluntad de otro es preciso que éste sepa la procedencia del acto de coacción sufrido.

Otro inconveniente del uso de *ciberproxies* radica en cómo el Estado los selecciona y controla cuando los instrumentaliza. La existencia de intereses divergentes entre ambas partes puede llevar a la deslealtad del *proxy*, ocasionando perjuicios económicos o políticos para el propio actor que los emplea –un hecho agravado si

tenemos en cuenta que estos *proxies* operan generalmente en ámbitos donde el Estado ni puede ni quiere intervenir.

El beneficio de los *proxies* está en su capacidad para actuar de forma encubierta, aunque esa misma falta de transparencia es lo que limita al Estado patrocinador a la hora de verificar sus antecedentes y confiabilidad. La literatura académica destaca que el control sobre los *proxies* se complica aún más si el Estado no cuenta con mecanismos efectivos para sancionar la deslealtad, o si existen estructuras descentralizadas que impidan un correcto cumplimiento de las órdenes jerárquicas (Popovic, 2015).

En el presente documento nos centraremos únicamente en dos actores que representan los dos polos distintos (activismo abierto y espionaje silencioso) de un mismo fenómeno, pero que no son tan diferentes si nos basamos en los fines que persiguen y en la instrumentalización que de ellos realizan los Estados.

En términos generales, el hacktivismo y las APT difieren en motivación, métodos y grado de respaldo estatal. Así, mientras que, el hacktivismo es movido por un contexto político-social (protesta, activismo, causas morales), las APT se centran en el espionaje estratégico y la obtención de una ventaja económico-militar.

Operacionalmente, las APT actúan a través del sigilo y la persistencia, empleando *malwares* personalizados, puertas traseras y movimientos laterales; a diferencia de las acciones hacktivistas que suelen buscar la atención pública y que se centran generalmente en el ataque mediante DDosS a corto plazo.

Sin embargo, no es extraño observar como las APT actúan temporalmente como hacktivistas (cuando divulgan públicamente los datos que exfiltran para provocar un impacto político) y como las hacktivistas son instrumentalizadas por los Estados para lograr sus fines estratégicos.

A nivel organización, hacktivistas y APT también presentan divergencias: los hacktivistas generalmente actúan de forma descentralizada, espontánea, incluso anónima, y sin mando unificado. Por su parte, las APT suelen ser equipos estructurados, muchas veces integrados en una organización mayor (un ejército, agencia de inteligencia o grupo criminal), con una jerarquía definida y una financiación considerablemente más potente (CyberZaintza, 2021).

Precisamente, la diferencia de recursos y de capacitación técnica sugiere un vínculo más estrecho de las APT con los Estados que los grupos hacktivistas. Pese a todo, las líneas que separan ambos conceptos se vienen difuminado recientemente en vistas a la constatación de que algunos grupos hacktivistas prorrusos vienen recibiendo el apoyo encubierto del Estado, o actúan alineados con la agenda estatal, borrando así la hasta ahora distinción clara entre "*hackers* activistas" y "operativos estatales" (Muncaster, 2024).

De hecho, no es descartable que, ciertos grupos hacktivistas en realidad estén formados o respaldados por APT's o, directamente, por actores estatales. Un ejemplo, lo encontraríamos en "XakNet Team", "Infoccentr" y "CyberArmyofRussia_Reborn", grupos hacktivistas prorrusos que según Mandiant se constituyen como actores de

ciberamenazas patrocinados por la Dirección Principal de Inteligencia de Rusia (GRU) a través de la APT44 (Mandiant, 2022).

A lo largo de la última década se han documentado múltiples casos en que los Estados han recurrido tanto a grupos APT propios como a colectivos hacktivistas (o sus identidades) para llevar a cabo operaciones de ciberespionaje, sabotaje en conflictos y manipulación política.

Un ejemplo paradigmático que ilustra la interdependencia de ambos conceptos, lo encontramos en las elecciones de EE.UU. de 2016, cuando "*DCLeaks*" y "*Guccifer 2.0*", dos identidades vinculadas a la Dirección Principal de Inteligencia de Rusia (*Glavnoe Razvedyvatel'noe Upravlenie*, GRU), robaron los correos del Partido Demócrata y los difundieron haciéndose pasar por "hacktivistas estadounidenses patriotas" (DOJ, 2018).

A raíz de la guerra de Ucrania, no es extraño encontrar la interdependencia entre hacktivistas y APT rusas, grupos como *Killnet, NoName057(16), Anonymous Sudan* que han atacado sitios web gubernamentales y empresas occidentales en apoyo a la narrativa del Kremlin muestran que, si bien estos grupos se autodenominan "activistas espontáneos", lo cierto es que, sospechosamente actúan de forma coordinada con la acción estatal rusa (Van Der Walt, 2025).

Sin embargo, Rusia no es el único actor estatal que emplea APT y hacktivistas para desplegar su poder. Otros Estados como China, Corea del Norte o Irán también han sido acusados durante años de conducir de esta forma sus actividades ofensivas en el ciberespacio.

Concretamente, China ha sido acusada durante años de patrocinar vastas campañas de espionaje cibernético a través de unidades militares y *hackers* a sueldo, como los del grupo APT1, considerados por Mandiant en 2013, como la Unidad 61398 del Ejército Popular de Liberación chino.

Las operaciones de APT chinas suelen centrarse en objetivos estratégicos (industrias aeroespaciales, energéticas, telecomunicaciones, defensa, etc.) y se consideran parte de la inteligencia estatal china, pero a diferencia de Rusia, en las estrategias chinas, el uso del hacktivismo no es tan prominente.

El gobierno ha tolerado e incluso inspirado a "*hackers* patrióticos" chinos en algunos conflictos, siendo un ejemplo de ello la "*Red de Hackers Honker*", una comunidad de *hackers* fuera de control gubernamental –según fuentes chinas— que ha atacado a actores adversarios de China durante disputas territoriales o incidentes diplomáticos.

Irán por su parte, sí ha mostrado una tendencia a instrumentalizar grupos de *hackers* supuestamente activistas para realizar operaciones de represalia contra sus adversarios, a la vez que desarrolla sus propias APT. Un ejemplo significativo de ello fueron los ataques DDoS contra bancos estadounidenses en 2012-2013, en represalia por las sanciones occidentales: una entidad que se presentaba como hacktivistas religiosa y autodenominada "*Cyber Fighters of Izz ad-Din al-Qassam*" se atribuyó la ofensiva alegando un sentimiento de indignación por un video antislámico (CFR, 2012).

Las agencias de inteligencia estadounidenses concluyeron posteriormente que se trató de una operación orquestada por Irán (probablemente su Guardia Revolucionaria) como respuesta a las medidas adoptadas contra su programa nuclear. De hecho, en 2016 el Departamento de Justicia de EE.UU. imputó a siete iraníes vinculados al Cuerpo de la Guardia Revolucionaria Islámica (IRGC) por estos ataques.

Otro ejemplo lo encontraríamos en el ataque "*Shamoonj*" de 2012 del grupo "*Cutting Sword of Justice*", un supuesto grupo hacktivista que borró los datos de 30.000 ordenadores de la petrolera saudí Aramco, pero que posteriormente los analistas atribuyeron a una operación del Estado iraní en respuesta a la ofensiva de *Stuxnet* y las tensiones regionales.

Corea del Norte, pese a su aislamiento, también ha logrado construir una de las amenazas cibernéticas más activas, principalmente para recaudar fondos y generar desestabilización en sus adversarios geopolíticos. Su grupo APT más notable, *Lazarus Group* (vinculado al APT38) ha robado cientos de millones mediante ataques a entidades bancarias.

Otro caso que ilustra la instrumentalización de las campañas activistas por parte de los Estados lo encontramos también en una de sus actuaciones, el *hackeo* a Sony Pictures en 2014, cuando un grupo denominado "*Guardians of Peace*" exfiltró datos confidenciales y destruyó sistemas de Sony en aparente represalia por la película satírica sobre el líder norcoreano "*The Interview*". (FBI, 2014).

Corea del Norte muestra el paradigma de la instrumentalización directa, sus *hackers* son agentes del Estado que en ocasiones asumen nombres de grupos ficticios para difundir sus mensajes o justificar sus ataques, pero a diferencia de otros Estados, los norcoreanos suprimen absolutamente la distinción entre APT y aparato estatal, manteniendo la cobertura únicamente en la narrativa pública de cara al exterior.

Por su parte, en las potencias occidentales obviamente también se emplean capacidades cibernéticas ofensivas para atacar otros Estados. Quizás el caso más relevante sea la operación "Olympic Games" atribuida a las agencias NSA y la unidad 8200 (no oficialmente reconocida), en la cual Estados Unidos e Israel desarrollaron el malware *Stuxnet* para sabotear las centrifugadoras nucleares de Irán alrededor del año 2010 (The Guardian, 2017).

Sin embargo, en Occidente, si bien existen entidades APT sustentadas por los Estados para actuar ofensivamente en campañas de espionaje, la instrumentalización de grupos hacktivistas para ocultar sus acciones es prácticamente inexistente. De hecho, únicamente podemos encontrar un caso donde un grupo hacktivista occidental vincula su actividad a la capacidad ciberofensiva de un Estado: el "*IT Army of Ukraine*".

Este caso es especialmente controvertido, pues el apoyo estatal público por parte del gobierno ucraniano viola abiertamente las normas recientemente acordadas sobre la conducta de los Estados en el ciberespacio, así como las posiciones de política exterior de los miembros de la OTAN (Healey y Grinberg, 2022).

Si utilizamos la tabla "Espectro de la responsabilidad" de Healey y Grinberg (2022), donde correlacionan la actividad de los grupos en función del grado de

responsabilidad del Estado para con su *ciberproxy*, podemos ver como el apoyo del Gobierno ucraniano al *IT Army of Ukraine* comenzó al menos como "coordinado por el Estado (nivel 6)", (cuando el Ministro ucraniano de Transformación Digital, Mijailo Fedorov llamó abiertamente a voluntarios hacktivistas de todo el mundo para que apoyaran a Ucrania en el frente digital) hasta llegar incluso a "alentado por el Estado (nivel 4)".

Tabla 1: *Espectro de la responsabilidad del Estado.*

Posición estatal	Relación Estado-*proxy*
1. Prohibido por el Estado.	El gobierno nacional ayudará a detener un ataque de terceros.
2. Prohibición estatal pero inadecuada.	El gobierno nacional coopera, pero es incapaz de detener el ataque de terceros.
3. Ignorado por el Estado.	El Gobierno nacional conoce los ataques de terceros, pero no está dispuesto a tomar ninguna medida oficial.
4. Fomentado por el Estado.	Terceros controlan y dirigen el ataque, pero el gobierno nacional los fomenta como una cuestión política.
5. Conformado por el Estado.	Terceros controlan y dirigen el ataque, y el Estado proporciona cierto apoyo.
6. Coordinado por el Estado.	El gobierno nacional coordina el ataque de terceros, por ejemplo, sugiriendo detalles operativos.
7. Ordenado por el Estado.	El gobierno nacional ordena a terceros que lleven a cabo el ataque en su nombre.
8. Dirigido, pero no reconocido por el Estado.	Elementos fuera de control de las fuerzas cibernéticas del gobierno nacional llevan a cabo el ataque ordenado.
9. Ejecutado por el Estado.	El gobierno nacional lleva a cabo el ataque utilizando fuerzas cibernéticas bajo su control directo.
10. Integrado en el Estado.	El gobierno nacional ataca utilizando proxies integrados y fuerzas cibernéticas gubernamentales.

(Healey, 2022).

Especialmente, en los conflictos geopolíticos es donde vemos una convergencia más acelerada entre el hacktivismo y las operaciones estatales. En el caso de la guerra de Ucrania, tres años después del inicio del conflicto y, pese a que el número de actores hacktivistas ha disminuido considerablemente (de más de 130 grupos en 2024 a sólo unos 80 grupos en 2025), podemos seguir observando como ambos bandos mantienen un cruce de ciberataques destructivos, coordinados con su campaña militar y apoyados en sus actuaciones por "hackers patrióticos" (Cyberknow, 2025).

En el bando ucraniano, el *IT Army of Ukraine* sigue vigente como la fuerza hacktivista más importante de Ucrania, movilizando aún a voluntarios dentro y fuera del país para atacar las infraestructuras rusas, efectuar contrapropaganda y apoyar misiones de inteligencia. En el periodo 2023-2024, se le atribuye, por ejemplo, la caída temporal

de servicios de Internet en zonas ocupadas por Rusia y el continuo despliegue de campañas de DDoS contra entidades rusas de alto perfil (Optiv, 2023).

Del lado prorruso, el grupo más prominente en la actualidad es *NoName057(16)*, un grupo vinculado al GRU, que actúa en coordinación con la agenda del Kremlin, al seleccionar objetivos en sintonía con los intereses estratégicos rusos y que se considera a sí mismo una suerte de "brazo ciberespontáneo" permanente del Ejército ruso.

Tabla 2: *Casos cronológicos de instrumentalización estatal del hacktivismo.*

Año	***Estado***	***Grupo hacktivista***	***Característica***	***Nivel de vinculación estatal (Healey & Grinberg).***
1998-1999	Kosovo	Hackers patrióticos	Primer conflicto con intervención hacktivista notable.	Ignorado / Espontáneo
1999	China	Red Honker	Hackers patrióticos activos en conflictos territoriales. Campañas de espionaje industrial y ciberataques a infraestructuras críticas.	Fomentado / Conformado
2012-2013	Irán	Cyber Fighters of Izz ad-Din al-Qassam	Ataques DDoS a bancos de EE.UU. como represalia por sanciones. Operación Shamoon contra Aramco con borrado masivo.	Coordinado / Ordenado
2014	Corea del Norte	Lazarus Group	Ciberataques para financiación estatal. Ataque a Sony Pictures (2014) como represalia simbólica	Ejecutado / Integrado
2022-presente	Rusia	Killnet/ Cyber Army of Russian Reborn/ NoName057(16)	Grupos hacktivistas coordinados con la estrategia rusa en la guerra de Ucrania. Ataques DDoS.	Coordinado / Fomentado
2022-presente	Ucrania	IT Army of Ukraine	Convocatoria pública del gobierno para hacktivismo contra Rusia. DDoS, sabotaje y propaganda pro-Ucrania.	Coordinado / Fomentado

4. EL FUTURO DE LOS GRUPOS HACKTIVISTAS.

La supervivencia de los grupos hacktivistas indica que el hacktivismo integrado en la guerra ha llegado para quedarse, al menos mientras dure el conflicto subyacente y los Estados en conflicto encuentren útil esa capa de acción descentralizada. Es más, el panorama hacktivistas actual nos lleva a observar como el hacktivismo está traspasando la frontera del DDoS y adentrándose en ataques más sofisticados propios de las APT, como son los ataques a sistemas SCADA y de control industrial (ICS) de infraestructuras críticas[4].

El hecho de que grupos pertenecientes al ecosistema hacktivista prorruso, como *Z-Pentest Alliance* o *Sector 16,* vengan realizando activamente intrusiones a plantas energéticas, instalaciones de agua potable e industrias en general, refleja no solamente una maduración y estatalización del fenómeno hacktivista, sino también la existencia de unos riesgos cada vez más físicos de sus acciones (Antoniuk, 2024).

La reducción del número de grupos hacktivistas del entorno prorruso sugiere que la efervescencia inicial ha dado paso a una selección natural donde sobreviven los colectivos con mejor apoyo, organización y protección. Un fenómeno que se traduce en operaciones más eficaces y coordinadas, aunque también más predecibles al estar alineadas con la agenda estatal rusa.

Al mismo tiempo, la persistencia de ataques diarios indica que la guerra cibernética de baja intensidad se ha vuelto rutinaria. Los DDoS constantes mantienen una presión psicológica y propagandística sobre las poblaciones objetivo (recordando diariamente la presencia del conflicto), mientras que, la adopción de *ransomware* y los ataques a las industrias eleva el potencial de daño real a infraestructuras críticas, desdibujando la línea entre el hacktivismo y ciberterrorismo –un hecho que puede terminar por derivar en respuestas más contundentes por parte de los Estados víctimas y posibilidades de escalada en los conflictos.

Otro hecho de relevancia es el desarrollo notable en las alianzas emergentes entre causas hacktivistas que transciende el teatro de operaciones más allá de Ucrania e implica a terceros países. Un ejemplo, es la reciente alianza entre hacktivistas prorrusos y propalestinos, que une causas geopolíticas aparentemente distintas bajo una narrativa de ataque común hacia Occidente.

Las tensiones globales de 2024 (incluida la guerra de Gaza) crearon un extraño frente unido de hacktivista. Los grupos rusos (especialmente *NoName057(16)*) comenzaron a coordinar operaciones con colectivos vinculados a Oriente Medio (como *Mr. Hamza* o *Anonymous Guys*), y sincronizaron sus ataques bajo la bandera de la unión "*Holy League*" contra países que percibían como adversarios compartidos, como es el ejemplo de Francia.

Este tipo de alianzas son conocidas en España, y particularmente, por la Guardia Civil, ya que, en julio de 2024, la Institución fue objetivo directo de una de campaña de ciberataques conjuntos, "*#FuckGuardiaCivil*", que respondía a una iniciativa promovida

[4] Sistema centralizado que permite supervisar, controlar y recopilar datos de procesos y dispositivos en tiempo real.

por el grupo *NoName057(16),* para "vengarse de las autoridades españolas" que habían detenido a tres personas en Manacor (Mallorca), Huelva y Sevilla, sospechosas de participar en ciberataques contra entidades públicas y empresas estratégicas de España y otros países de la OTAN.

De hecho, en abril de 2025, ya se registró una nueva alianza conformada, entre otros, por los grupos *Keymous+, Mr Hamza, ¡Alixsec y NoName057(16)* para atacar a Polonia, Alemania, Francia, Italia y España bajo el lema "*Operation Hack For Humanity V2!*".

Tan solo en el caso español, el primer día de la campaña "Operation Hack For Humanity V2!" se registraron más de 30 ataques a empresas y sitios web gubernamentales, siendo los grupos más activos en el ataque *Mr Hamza*, *NoName057(16)*, *TwoNet* y *Keymous+*.

La frecuencia con la que se viene produciendo esta convergencia en los últimos meses demuestra que, el fenómeno cada día es más internacional y está más interconectado. Las alianzas entre grupos hacktivistas se han solidarizado entre sí, trascendiendo las fronteras del conflicto ruso-ucraniano con un único objetivo: ampliar sus acciones hacia el enemigo común occidental.

El hecho de que países de la OTAN, como Francia, Italia o la propia España, puedan convertirse en objetivos de los *hackers* patrióticos rusos podría llegar a producir una escalada en el conflicto, especialmente si uno de sus ataques lograse dañar severamente una infraestructura crítica, la guerra cibernética de baja intensidad podría obtener una respuesta más firme de lo usual.

5. CONCLUSIONES

El análisis del hacktivismo y su relación con los Estados demuestra que, este fenómeno ha evolucionado desde la protesta digital hacia una instrumentalización estatal con implicaciones geopolíticas y estratégicas. La frontera entre activismo, cibercriminalidad y operaciones estatales es cada vez más difusa, especialmente en conflictos como la guerra de Ucrania, donde se ha observado una creciente instrumentalización de los grupos hacktivistas por parte de las fuerzas gubernamentales en la defensa de sus intereses nacionales.

Ciertamente, el conflicto entre Rusia y Ucrania ha marcado un punto de inflexión en el uso del ciberespacio como campo de batalla, donde tanto actores estatales como no estatales han participado activamente en ataques de denegación de servicio (DDoS), ciberespionaje y sabotaje de infraestructuras críticas.

El presente estudio, desarrollado a través del estudio de los casos más destacados en el escenario internacional, ha permitido establecer una distinción entre los *hackers* cívicos y los *hackers* patrióticos. Mientras que, los primeros abrazan causas nihilistas o socialmente conflictivas, los segundos son utilizados por los Estados como una herramienta encubierta en conflictos internacionales, lo cual supone una externalización de las capacidades cibernéticas gubernamentales y ofrece una serie de ventajas

estratégicas: negación plausible de responsabilidad, prolongación de situaciones de tensión o la reducción de costes políticos y económicos.

En síntesis, podríamos decir que, los Estados han aprendido a aprovechar el hacktivismo como un arma adicional, ya sea fingiéndose hacktivistas para desinformar o exfiltrando datos o animando a sus simpatizantes a lanzar ciberataques en masa contra su enemigo.

Esta instrumentalización plantea, sin embargo, serios desafíos a nivel estratégico. La progresiva sofisticación de unos ataques que han pasado del vandalismo digital a operaciones más avanzadas contra infraestructuras críticas no hace sino incrementar seriamente las posibilidades de represalias por parte de los Estados afectados y aumentar el riesgo potencial de escalada en los conflictos asimétricos.

Además, la convergencia entre las APT y los hacktivistas pone en cuestión las normativas internacionales vigentes, ya que, los ataques perpetrados por actores *proxies* difuminan la responsabilidad estatal y dificultan la aplicación de medidas de disuasión o represalias directas. Especialmente, cuando los colectivos hacktivistas parecen evolucionar hacia un nuevo panorama de alianzas capaz de aglutinar a grupos hacktivistas con agendas geopolíticas diversas para atacar a los países occidentales.

La seguridad cibernética de los Estados debe adaptarse a una nueva realidad en la que los grupos hacktivistas juegan un papel clave en la proyección del poder estatal. Las democracias occidentales, tradicionalmente más reacias a utilizar este tipo de tácticas, se deben enfrentar al dilema de cómo responder de manera efectiva sin comprometer sus valores.

La tendencia actual no solamente muestra una clara evolución del hacktivismo hacia una vinculación cada vez mayor con los intereses estatales del Gobierno que les sustenta, sino que también refuerza la idea de que el ciberespacio continuará adquiriendo una mayor importancia en los conflictos del futuro. Casos como el de Rusia, donde grupos como *Killnet* o *NoName057(16)* han reivindicado operaciones cibernéticas coincidentes con los intereses geopolíticos del Kremlin —especialmente durante la guerra en Ucrania—, o el de Irán, con colectivos como *Tapandegan*, cuya retórica oposicionista no impide sospechas de coordinación indirecta con agendas estatales, ejemplifican esta deriva, evidencian un progresivo desdibujamiento entre actores no estatales y estatales en el ámbito digital, donde el hacktivismo deja de ser exclusivamente una forma de disidencia ciudadana para convertirse, en ciertos contextos, en una herramienta informal de proyección del poder estatal.

6. REFERENCIAS BIBLIOGRÁFICAS

Antoniuk, D. (2024). *Cybervolk: Hacktivists from India and Russia collaborate on ransomware attacks*. The Record. https://therecord.media/cybervolk-india-hacktivists-russia-ransomware

Antoniuk, D. (2024). *Cybervolk: Hacktivists from India and Russia collaborate on ransomware attacks*. The Record. https://therecord.media/cybervolk-india-hacktivists-russia-ransomware

Auty, C. (2004). Political hacktivism: Tool of the underdog or scourge of cyberspace? *Aslib Proceedings, 56*(4), 212-221.

Bartlett, J. (2015). *The dark net: Inside the digital underworld*. Melville House.

CFR (2012). *Denial of service attacks against U.S. banks in 2012–2013*. Council on Foreign Relations (CFR). https://www.cfr.org/cyber-operations/denial-service-attacks-against-us-banks-2012-2013

Coleman, G. (2014). *Hacker, hoaxer, whistleblower, spy: The many faces of Anonymous*. Verso Books.

Cyberknow (2025). *Russia-Ukraine war: Hacktivist update*. https://cyberknow.substack.com/p/russia-ukraine-war-hacktivist-update

CyberZaintza (2021). *Grupo APT*. https://www.ciberseguridad.eus/ciberglosario/grupo-apt

Dahan, M. (2013). Hacking for the homeland: Patriotic hackers versus hacktivists. *International Conference on Information Warfare and Security*, 51–VII. Academic Conferences International Limited. https://search.proquest.com/docview/1549245919

Denning, D. E. (2001). Activism, hacktivism, and cyberterrorism: The internet as a tool for influencing foreign policy. En J. Arquilla & D. Ronfeldt (Eds.), *Networks and netwars: The future of terror, crime, and militancy* (pp. 239-288). RAND Corporation.

DOJ (2018). *Grand jury indicts 12 Russian intelligence officers for hacking offenses related to the 2016 election*. U.S. Department of Justice. https://www.justice.gov/archives/opa/pr/grand-jury-indicts-12-russian-intelligence-officers-hacking-offenses-related-2016-election

Expósito Guisado, J. (2023). *Ciberproxies: las APT como factor de riesgo futuro*. Instituto Español de Estudios Estratégicos (IEEE). *Boletín IEEE*, (32), 815-831.

FBI (2014). *Update on Sony Investigation*. Federal Bureau of Investigation (FBI), Washington, D.C. https://www.fbi.gov/news/press-releases/update-on-sony-investigation

Fox, A. C. (2019). *Conflict and the need for a theory of proxy warfare*. *Journal of Strategic Security, 12*(1), 44–71. JSTOR. www.jstor.org/stable/26623077

Goode, L. (2015). Anonymous and the political ethos of hacktivism. *Popular Communication, 13*(1), 74–86. https://doi.org/10.1080/15405702.2014.978000

Green, K. (2016). People's war in cyberspace: Using China's civilian economy in the information domain. *Military Cyber Affairs, 2*(1). https://doi.org/10.5038/2378-0789.2.1.1022

Healey, J., & Grinberg, A. (2022). *Patriotic hacking: No exception*. Lawfare. https://www.lawfaremedia.org/article/patriotic-hacking-no-exception

Hern, A. (2017). NSA contractor leaked US hacking tools by mistake, Kaspersky says. *The Guardian*. https://www.theguardian.com/technology/2017/oct/26/kaspersky-russia-nsa-contractor-leaked-us-hacking-tools-by-mistake-pirating-microsoft-office

Hunsinger, J., & Schrock, A. (2016). The democratization of hacking and making. *New Media & Society, 18*(4), 535–538. https://doi.org/10.1177/1461444816629466

Johnson, P., & Robinson, P. (2014). Civic hackathons: Innovation, procurement, or civic engagement? *Review of Policy Research, 31*(4), 349–357. https://doi.org/10.1111/ropr.12074

Jordan, T. (2002). *Activism! Direct action, hacktivism and the future of society*. Reaktion Books.

Jordan, T., & Taylor, P. A. (2004). *Hacktivism and cyberwars: Rebels with a cause?* Psychology Press.

Mandiant (2022). *GRU's rise: Telegram minions*. https://cloud.google.com/blog/topics/threat-intelligence/gru-rise-telegram-minions

Marín, F. (2023). *Hacktivismo al servicio del Estado: ciberproxies en Ucrania*. Documento de Opinión. Instituto Español de Estudios Estratégicos (IEEE).

Maurer, T. (2018). *Cyber Mercenaries: The state, hackers, and power*. Cambridge University Press.

Muncaster, P. (2024). *El hacktivismo: Evolucionando amenazas para las organizaciones*. WeLiveSecurity. https://www.welivesecurity.com/es/cibercrimen/el-hacktivismo-evolucionando-amenazas-organizaciones

Olson, P. (2012). *5 things every organization can learn from Anonymous*. Forbes. http://www.forbes.com/sites/parmyolson/2012/06/05/5-things-every-organization-can-learn-from-anonymous/

OPTIV (2023). *Russia/Ukraine Update - December 2023*. https://www.optiv.com/insights/discover/blog/russiaukraine-update-december-2023

Popovic, M. (2015). Fragile proxies: Explaining rebel defection against their state sponsors. *Terrorism and Political Violence*. https://doi.org/10.1080/09546553.2015.1092437

Rondeaux, C., & Sterman, D. (2019). *Twenty-first century proxy warfare: Confronting strategic innovation in a multipolar world since the 2011 NATO intervention*. New America. https://d1y8sb8igg2f8e.cloudfront.net/documents/Twenty-First_Century_Proxy_Warfare_Final.pdf

Sauter, M. (2013). "LOIC will tear us apart": The impact of tool design and media portrayals in the success of activist DDOS attacks. *American Behavioral Scientist, 57*(7), 983–1007. https://doi.org/10.1177/000276

Schrock, A. R. (2016). Civic hacking as data activism and advocacy: A history from publicity to open government data. *New Media & Society, 18*(4), 581–599. https://doi.org/10.1177/1461444816629469

Torres Soriano, M. (2017). Guerras por delegación en el ciberespacio. *Revista del Instituto Español de Estudios Estratégicos, (9)*, 15-36.

(2018). El hacktivismo como estrategia de comunicación de Anonymous al cibercalifato. *Cuadernos de Estrategia, (197)*, 197-224.

Van Der Walt (2025). *Reflecting on three years of cyber warfare in Ukraine*. *ComputerWeekly*. https://www.computerweekly.com/opinion/Reflecting-on-three-years-of-cyber-warfare-in-Ukraine

Vegh, S. (2005). *The media's portrayal of hacking, hackers, and hacktivism before and after September 11*. *First Monday*. http://uncommonculture.org/ojs/index.php/fm/article/view/1206/1126

Revista Científica del Centro Universitario de la Guardia Civil
Revista Logos Guardia Civil

Artículo de Investigación

PROTECCIÓN INTERNACIONAL Y SOBERANÍA: EL COMPLICADO BALANCE ENTRE DERECHOS INDIVIDUALES Y SEGURIDAD NACIONAL

Alejandro Gómez García
Capitán de la Guardia Civil
Master en Dirección Operativa de la Seguridad
Grado en Derecho
alejandrogomezg@guardiacivil.es
ORCID: https://orcid.org/0000-0003-0162-4213

Recibido 31/03/2025
Aceptado 28/04/2025
Publicado 27/06/2025

Cita recomendada: Gómez, A. (2025). Protección internacional y soberanía: el complicado balance entre derechos individuales y seguridad nacional. *Revista Logos Guardia Civil*, 3(2), p.p. 123-146.

Licencia: Este artículo se publica bajo la licencia Creative Commons Atribución-NoComercial-SinDerivadas 4.0 Internacional (CC BY-NC-ND 4.0)
Depósito Legal: M-3619-2023
NIPO en línea: 126-23-019-8
ISSN en línea: 2952-394X

ORCID: https://orcid.org/0000-0003-0162-4213

PROTECCIÓN INTERNACIONAL Y SOBERANÍA: EL COMPLICADO BALANCE ENTRE DERECHOS INDIVIDUALES Y SEGURIDAD NACIONAL

Sumario: 1. INTRODUCCIÓN. 2. ANÁLISIS TEÓRICO-METODOLÓGICO: ESTADOS, FRONTERAS Y PROTECCIÓN INTERNACIONAL. 2.1. Mapa conceptual del entorno fronterizo. 2.2. Migración y Asilo. 3. ANÁLISIS JURÍDICO: POSTURAS ENFRENTADAS Y RESPUESTA DE LOS TRIBUNALES. 3.1. Caso *Hirsi Jamaa contra Italia*: la génesis de una doctrina. 3.2. Caso *N. D. Y N. T. contra España*: Los límites a la protección. 3.3. Análisis comparativo: la compatibilización de una doctrina jurisprudencial dispar. 4. CONCLUSIONES.

Resumen: En el presente artículo se pretende analizar el estatus jurídico que ostentan, en la actualidad, algunos de los conceptos más relevantes dentro del ámbito de la protección de las fronteras nacionales, así como su contexto sociopolítico y su alcance jurídico, con el fin último de fundamentar e impulsar el desarrollo de un debate doctrinal tan candente en sus posturas como complejo en su contexto: Asegurar un adecuado balance entre la garantía de los Derechos Fundamentales de los individuos que transiten por las fronteras europeas y el ejercicio de las potestades soberanas consustanciales a los Estados. Así, en primer lugar, se realizará un examen pormenorizado de las nociones más importantes en el ámbito de la seguridad fronteriza, fijando el campo de estudio desde un punto de vista científico. Inmediatamente a continuación se estudiarán, desde una perspectiva jurídica, las implicaciones que han tenido los pronunciamientos más importantes efectuados por los órganos judiciales (fundamentalmente internacionales) que han entendido de la materia, así como la posición de la doctrina y la práctica internacional. Y finalmente, a la luz de los análisis expuestos, se ofrecerá una serie de conclusiones coherentes con los hallazgos efectuados.

Abstract: This article aims to analyze the current legal status of some of the most significant concepts within the field of national border protection, as well as their sociopolitical context and legal scope, with the ultimate goal of providing a foundation for, and promoting the development of, a doctrinal debate that is as contentious in its positions as it is complex in its context: ensuring an appropriate balance between guaranteeing the fundamental rights of individuals crossing European borders and the exercise of sovereign powers inherent to States. To this end, the following pages will firstly conduct a detailed examination of the fundamental concepts in the field of border protection, establishing the scope of study from a scientific perspective. Subsequently, from a legal perspective, the implications of the most significant rulings issued by judicial bodies (primarily international) that have adjudicated on the matter will be analyzed, alongside the positions of legal scholarship and international practice. Finally, in light of the analyses presented, a series of conclusions consistent with the findings will be offered.

Palabras clave: Derecho Internacional, Asilo, Soberanía, Fronteras, Inmigración.

Keywords: International Law, Asylum, Sovereignty, Borders, Immigration.

ORCID: https://orcid.org/0000-0003-0162-4213

ABREVIATURAS

AN: Audiencia Nacional

ANP: Autoridad Nacional Palestina

CDFUE: Carta de los Derechos Fundamentales de la Unión Europea

CEDH: Convenio Europeo de los Derechos Humanos

IMO: *International Maritime Organization* – Organización Marítima Internacional

SAR: *Search and Rescue* – Búsqueda y Rescate

SOLAS: *Security Of Life At Sea* – Seguridad de la vida en el mar

TEDH: Tribunal Europeo de los Derechos Humanos

TIJ: Tribunal Internacional de Justicia

TPA: Tribunal Permanente de Arbitraje

TPJI: Tribunal Permanente de Justicia Internacional

UE: Unión Europea

1. INTRODUCCIÓN

Tras la Sentencia del Tribunal Europeo de los Derechos Humanos (en adelante TEDH), Sección Tercera, de 3 de octubre de 2017, por la cual se condenó al Estado español, en el marco de la práctica del «rechazo en frontera», por vulneración del artículo 13 del Convenio Europeo de los Derechos Humanos (en adelante CEDH) y del artículo 4 de su Protocolo nº 4, disponiéndose el abono de sendas indemnizaciones a los demandantes N. D. (nacional maliense) y N.T. (nacional marfileño) por valor de 5 000 euros cada una; muchas fueron las voces que reclamaron un cambio total de rumbo en la política migratoria desarrollada por el Reino de España y, por extensión, en la política migratoria europea. En efecto, la noticia acaparó no pocos titulares en prensa[1], así como encendidos pronunciamientos de organizaciones no gubernamentales[2] e incluso de entidades de derecho público[3], en un país poco acostumbrado a seguir con tanto detalle la crónica judicial, y menos aún la de carácter internacional.

Y es que la situación no era para menos. La creciente preocupación por el contexto migratorio en la Unión Europea (en adelante UE) había ido dando lugar, con el paso de los años, al surgimiento de ciertos debates que, hasta ese momento, habían permanecido al margen de las dinámicas políticas, las cuales aceptaban como algo casi anecdótico el sostenido incremento de las cifras de nacionales de terceros países residentes en la Unión, cuyo número había aumentado más de un 10% en los tres años previos al referido pronunciamiento[4]. Por supuesto, al auge de este debate había contribuido también la llamada «Crisis de los Refugiados» de 2015, a causa de la cual centenares de miles de desplazados procedentes de Oriente Medio (mayoritariamente sirios) habían entrado en territorio europeo como consecuencia de la inestabilidad y la guerra en la región. Y, definitivamente, no ayudaría a disminuir la tensión en la sociedad europea el hecho de que algunos de los implicados en distintos actos terroristas que tuvieron lugar durante aquellos años (por ejemplo, los atentados de Ansbach y Berlín durante el año 2016 o, por supuesto, los atentados de París de 2015) fueran posteriormente identificados como refugiados o inmigrantes clandestinos, procedentes de Siria a través de la ruta mediterránea oriental.

Pero, por si lo descrito fuera poco, el porvenir reservaba una nueva sorpresa mayúscula que volvería a hacer girar con fuerza el guion de la política migratoria europea. En un hecho sin precedentes, el mismo TEDH que había liquidado la doctrina española sobre los rechazos en frontera revocaría su resolución de instancia y, en sentencia de Gran Sala de 13 de febrero de 2020, procedió a declarar, por una mayoría de 16 a 1, la plena legalidad de los rechazos en frontera. Después, llegó la pandemia. Y con ella también la reactivación de la ruta migratoria atlántica con destino a las Islas Canarias, así como un nuevo auge en general de los movimientos migratorios con destino a la Unión, que repuntarían desde las 125 226 entradas ilegales detectadas durante el año 2020 (Frontex,

---

[1] RTVE (3 de octubre de 2017), *El Tribunal Europeo de Derechos Humanos condena a España por dos "devoluciones en caliente" en Melilla*, https://www.rtve.es/noticias/20171003/tribunal-europeo-derechos-humanos-condena-a-espana-por-dos-devoluciones-caliente-melilla/1625420.shtml.

[2] Comisión Española de Ayuda al Refugiado (3 de octubre de 2017), *El Tribunal Europeo de DDHH condena a España por dos 'devoluciones en caliente'*, https://www.cear.es/noticias/tribunal-europeo-ddhh-condena-espana-dos-devoluciones-caliente-nuestra-frontera-sur/.

[3] Consejo General de la Abogacía Española (3 de octubre de 2017), *La Abogacía reitera la ilegalidad de las devoluciones en caliente, tras la condena del TEDH*, https://www.cear.es/noticias/tribunal-europeo-ddhh-condena-espana-dos-devoluciones-caliente-nuestra-frontera-sur/.

[4] Datos de Eurostat, https://ec.europa.eu/eurostat/databrowser/view/migr_pop1ctz/default/table?lang=en.

ORCID: https://orcid.org/0000-0003-0162-4213

2021, p. 14) hasta las 380 227 de 2023 (Frontex, 2024, p. 1). Hoy, la inmigración ocupa un espacio predominante entre las mayores preocupaciones de los ciudadanos del continente. Así, el último «eurobarómetro», publicado en noviembre de 2024, destaca la inmigración como la segunda prioridad en cuanto a las áreas en las que la UE debe tomar medidas en opinión de los europeos, postura que apoya un 29% de los encuestados (Comisión Europea, 2024, p. 14), únicamente por detrás de la Seguridad y la Defensa.

Sin embargo, y pese a que la Comisión Europea no duda en responder a tales preocupaciones señalando de forma recurrente los «avances» que se van realizando en materia de «gestión de fronteras» (Comisión Europea, 2022, p. 5), lo cierto es que, cuando en la ecuación se introduce el factor de la salvaguarda de los derechos fundamentales, la situación se complica. Y es que las políticas orientadas a reforzar el control fronterizo, desarrolladas en base a los objetivos de robustecer el sistema sobre el que descansa la seguridad nacional y garantizar la soberanía de los Estados, conllevan medidas destinadas a obstaculizar la inmigración ilegal que, por su propia naturaleza, inciden en los derechos de la población concernida. Y, conforme a las normas básicas que rigen el Estado de derecho, en el caso de que esa afectación no sea idónea, coherente y proporcional con respecto a los fines lícitos perseguidos, podría suponer una intromisión ilegal en núcleo más esencial de los derechos fundamentales, especialmente cuando condicionaran ámbitos clave como el derecho de asilo. El presente artículo de investigación tiene como objetivo analizar este delicado equilibrio, revelando los puntos de fricción entre ambas realidades en conflicto a través del examen detallado de la jurisprudencia nacional e internacional; así como clarificando, tanto como sea posible, hasta dónde puede llegar la legalidad en las actuaciones de los guardias civiles en cuanto a su condición de guardias de fronteras.

2. ANÁLISIS TEÓRICO-METODOLÓGICO: ESTADOS, FRONTERAS Y PROTECCIÓN INTERNACIONAL

2.1. MAPA CONCEPTUAL DEL ENTORNO FRONTERIZO

2.1.1. El concepto de frontera

El término «frontera» posee casi tantas acepciones como ramas de la ciencia han contemplado el estudio de cualquier concepto derivado de la noción intuitiva de «límite». Desde la matemática hasta la ciencia política, pasando por las relaciones internacionales o el Derecho. Afirma Sanz Donaire (2023, p. 254) que el término en cuestión procede del término latino clásico *frons*, cuyo significado referiría a los de «frente» o «fachada», y ofrecería ya de primeras una idea del contexto antagonista o distintivo con el que se desarrollaría desde su formulación, fuertemente vinculado al ámbito militar, a la protección frente a lo extraño, lo exterior. Efectivamente, las fronteras han estado ligadas al conflicto y a la confrontación desde el Tratado de Mesilim, considerado el «tratado más antiguo del que existen registros» (Doebbler, 2018, pp. 374-375), que no era sino un convenio que regulaba el reconocimiento de los límites entre varios reinos mesopotámicos en torno al 2500 a. C. Y en tal sentido se expresaría también Curzon (1907) en los albores del estudio científico de las Relaciones Internacionales, cuando afirmó que las tensiones fronterizas han sido el factor más importante en los conflictos entre Estados (p. 4).

En cualquier caso, es sobre tales antecedentes etimológicos que se asientan las actuales concepciones de frontera, de entre las cuales destaca, por su potencia discursiva la del Diccionario del Español Jurídico, que enuncia lo siguiente:

«Frontera (Derecho Internacional Público): *Línea que marca el límite exterior del territorio de un Estado, entendido como el espacio terrestre, marítimo y aéreo sobre el que ejerce su soberanía, lo que permite hablar de fronteras terrestres, marítimas y aéreas en función de la naturaleza física del espacio delimitado».*

2.1.2. Fronteras y soberanía

Conforme a las tesis de Lacan (1966), la comprensión de los conceptos se sustenta en el entendimiento de las relaciones que estos desarrollan con respecto a aquellas nociones previas que componen su significado, mediante una concatenación de referencias en lo que el psicoanalista francés conocía como «cadenas de significantes» (pp. 501-502). En tal sentido, y atendiendo a la definición expuesta en el epígrafe anterior, parece evidente que no podremos alcanzar un conocimiento satisfactorio de la realidad estudiada sin antes estudiar el otro concepto técnico que en ella se pone en juego: el de soberanía.

Al respecto de este concepto se ha escrito de forma muy prolífica. Desde que Juan Bodino realizara, en el siglo XVI, una primera aproximación en la que se intrincaban componentes nacionales, territoriales y teológicos, la noción de soberanía ha estado ligada a la existencia de un vínculo ajeno a la mera extensión física y social en la que se ejerce el poder, y que de alguna manera trasciende a lo estrictamente territorial. Quizás por ello no abundan las fuentes escritas de derecho internacional que ofrezcan de forma cristalina y universal una definición de soberanía. Uno de los pocos textos que pueden darnos alguna pista al respecto es la Convención de Montevideo, sobre Derechos y Deberes de los Estados, de 1933. Este tratado ofrece lo que, en la práctica, ha acabado por convertirse en una definición de soberanía, al establecer, en su artículo 1, los requisitos básicos para poder considerar a una entidad estatal como sujeto de Derecho Internacional:

1. Población permanente.
2. Territorio determinado.
3. Gobierno.
4. Capacidad de entrar en relaciones con los demás Estados.

Es destacable que, pese a que formalmente este tratado solo es aplicable al muy reducido elenco de estados que lo firmaron (se acordó en la Séptima Conferencia Internacional de los Estados Americanos, antecedente directo de la Organización de Estados Americanos), el mismo «ha recibido una adhesión general desde el punto de vista doctrinal» (Infante Caffi, 2016, p. 66), extendiéndose de forma paulatina sus postulados —bien por remisión directa o bien mediante referencia a una costumbre internacional apoyada en ellos— a una generalidad de actores internacionales entre los que se encuentra la propia Unión Europea[5].

[5] Véanse, por ejemplo, las Conclusiones del Consejo Europeo sobre el proceso de paz en Oriente Medio, de 20 de julio de 2015; o la resolución del Parlamento Europeo sobre el papel de la UE en el proceso de paz en Oriente Medio, de 10 de septiembre de 2015; en el marco de las cuales se promueve un camino hacia el reconocimiento de Palestina como entidad política («solución de dos Estados») sobre la base de una población permanente (a la que se refieren reiteradamente como «población palestina»), un territorio permanente (señalando su compromiso con las «fronteras de 1967»), un gobierno efectivo (encarnado en la «Autoridad Palestina», en adelante ANP, a la que se cita de forma expresa) y una capacidad para entrar en relaciones con otros Estados (citando y reconociendo los acuerdos alcanzados con la ya referida ANP).

ORCID: https://orcid.org/0000-0003-0162-4213

Igualmente, la jurisprudencia internacional ha ido perfilando el concepto de soberanía, siendo que, en ausencia de un título objetivo (por ejemplo, un tratado de límites suscrito y observado por todos los Estados afectados), se considera que un Estado es soberano sobre un territorio cuando este muestra su intención de serlo a través de medios idóneos para ello en Derecho Internacional (por ejemplo, una declaración unilateral) y, al mismo tiempo, cuando dicho Estado es capaz de ejercer de forma práctica dicha autoridad, a través del desarrollo efectivo de jurisdicción sobre el territorio (Sentencia del Tribunal Permanente de Justicia Internacional de 5 de abril de 1933, pp. 45-27 in fine, 46-28 in limine; Sentencia del Tribunal Internacional de Justicia de 17 de diciembre de 2002, párr. 134, p. 182-61; Laudo del Tribunal Permanente de Arbitraje de 9 de octubre de 1998, párr. 239, p. 268; entre otras).

Será en base a esta soberanía sobre la que se fundamentará el legítimo derecho de los Estados a la protección de sus fronteras, habitualmente amparado bajo las normas tradicionales del derecho consuetudinario internacional y la referencia al artículo 51 de la Carta de las Naciones Unidas; y que en el caso europeo trascenderá al ámbito nacional, a la vista de la obligación internacional que supone para sus signatarios el acuerdo de Schengen.

2.2. MIGRACIÓN Y ASILO

Por otra parte, al manejar los conceptos relacionados con los derechos ostentados por los particulares dentro del ámbito fronterizo, no es inhabitual que se produzcan ciertos equívocos (por ejemplo, al respecto de las nociones de «inmigrante» y «refugiado»), lo que hace aconsejable estudiar breve pero rigurosamente tal entorno jurídico, especialmente en lo relativo al contenido y alcance de la protección internacional.

2.2.1. El derecho de asilo y la protección subsidiaria

El término «asilo», procede del griego *ásylon*, vocablo cuya traducción se acerca a la de «sitio inviolable». En su concepción inicial se trataba de la condición que se dispensaba al *hieron*, una suerte de espacios especiales situados dentro de los *témenos*, áreas consagradas a los dioses (Harris Díez, 2011, p. 70), las cuales quedaban fuera de la jurisdicción del Estado, «pudiendo así convertirse en un refugio para individuos perseguidos, esclavos fugados u hombres políticos» (Zaidman y Schmitt-Pantel, 2002, p. 45). Sobre este antecedente se formará el dogma cristiano del «asilo en sagrado», estatus de inmunidad conferido tradicionalmente a los lugares de culto con el fin de proteger a los necesitados y redimir a los criminales arrepentidos (Golmayo, 1866, pp. 88-89), de la que posteriormente derivaría a su vez el concepto moderno del «derecho de asilo».

Este concepto moderno del derecho de asilo se establecerá fundamentalmente a través de la proclamación de dos textos: la Convención de Ginebra sobre el Estatuto de los Refugiados de 1951 (en adelante Convención de Ginebra), que conforma la figura del refugio; y su Protocolo de 1967, que generaliza tal protección, inicialmente creada para un elenco muy reducido de beneficiarios. Mediante la conjunción de estos dos textos se puede alcanzar una definición única que reconoce como refugiado o beneficiario de asilo a toda aquella persona que:

«…Debido a fundados temores de ser perseguida por motivos de raza, religión, nacionalidad, pertenencia a determinado grupo social u opiniones políticas, se encuentre

fuera del país de su nacionalidad y no pueda o, a causa de dichos temores, no quiera acogerse a la protección de tal país; o que, careciendo de racionalidad y hallándose fuera del país donde antes tuviera su residencia habitual, no pueda o, a causa de dichos temores, no quiera regresar a él».

Por otra parte, siendo tal la definición general, lo cierto es que los distintos modelos de protección de los derechos fundamentales existentes han desarrollado toda una batería de normas que amplían y clarifican el contenido de este derecho. En el ámbito de la Unión Europea, esta labor es realizada a través de la Directiva 2011/95/UE, que establece aspectos nucleares dentro del propio proceso de obtención de la condición de refugiado como son los criterios de valoración de las circunstancias que pueden ser consideradas como persecución, al tiempo que (y esto es enormemente relevante) se introduce en el derecho comunitario la denominada «protección subsidiaria», una garantía que salvaguarda la situación jurídica de aquellos nacionales de terceros países y apátridas que, «sin reunir los requisitos para obtener el asilo, […] se den motivos fundados para creer que si regresasen a su país de origen […] se enfrentarían a un riesgo real» (art. 4). Dicha protección subsidiaria —que, junto con el derecho de asilo, forma lo que en la terminología comunitaria se denomina de forma genérica como «protección internacional»— está pensada para extender la indemnidad propia del estatuto del refugiado a personas en riesgo de ser condenadas a pena de muerte, sometidas a tortura o, incluso, de sufrir las consecuencias de un conflicto bélico.

En cualquier caso, toda la normativa referida establece explícitamente la inaplicabilidad de tal protección a aquellos que puedan considerarse autores de graves delitos internacionales (criminales de guerra, genocidas, etc.), prófugos de delitos comunes de gravedad o personas que representan un peligro para la seguridad del país de acogida.

2.2.2. Derechos aplicables a los beneficiarios de protección internacional

Toda protección internacional otorga una serie de derechos mínimos a sus beneficiarios, si bien determinados aspectos accidentales de aquellos (plazos, extensión, etc.) pueden variar ligeramente en función de si la figura concedida es la de asilo (más protegida) o la de protección subsidiaria (menos protegida). Además, una parte importante de estos derechos serán también ejercitables no solo por aquellos que hayan sido oficialmente reconocidos como beneficiarios de cualquier tipo de protección, sino que la normativa europea reconoce su aplicabilidad también para los meros solicitantes, en tanto en cuanto no se resuelva su expediente[6]. En cualquier caso, existen dos derechos básicos que se hallan unidos de forma intrínseca a cualquiera de las formas de protección internacional —incluyendo a los solicitantes— y cuya naturaleza será determinante en el conflicto entre los derechos individuales y la seguridad nacional: la tutela judicial efectiva y la no devolución.

2.2.2.1. Derecho a la tutela judicial efectiva

El derecho a la tutela judicial efectiva, entendido como la garantía que ostentan los ciudadanos «del acceso a la jurisdicción, de la tramitación del proceso, de la resolución [razonable] del caso y de la ejecución de la sentencia» (Carrasco Durán, 2020, p. 20) en el

[6] Por ejemplo, y conforme a lo establecido en la Directiva 2013/33/UE, el derecho a acceder a la atención sanitaria (art. 19), a las ayudas públicas (art. 18) o al mercado laboral (art. 15).

ORCID: https://orcid.org/0000-0003-0162-4213

marco de un sistema judicial justo e imparcial, no se constituye como una garantía específica del derecho de asilo, sino que su alcance es universal, y como tal está recogida en la Constitución Española (art. 24) y en la Carta de los Derechos Fundamentales de la UE (art. 47), bajo la referencia permanente de los derechos al proceso equitativo (art. 6) y al recurso efectivo (art. 13).

Sin embargo, su impacto en el ámbito del derecho de asilo ha sido notable, hasta el punto de que la Directiva 2013/32/UE garantiza (art. 46) el acceso a recurso en los procedimientos de asilo, estableciendo explícitamente que este debe sustanciarse ante un órgano «jurisdiccional». Así, una de las alegaciones más recurrentes a la hora de impugnar las acciones del Estado en el ámbito fronterizo ha sido una presunta ausencia o precariedad en el acceso a los recursos judiciales. En tal sentido, y dentro del ámbito europeo, la garantía jurisdiccional última de la tutela judicial efectiva se ha canalizado —previo agotamiento de las instancias nacionales— mediante recurso al TEDH por violación del artículo 13 del CEDH[7]. Sin embargo, la jurisprudencia de este tribunal es clara al respecto del mismo: para poder hallar una transgresión del artículo 13, previamente debe existir una reclamación que de forma plausible plantee la violación de cualquier otro de los derechos garantizados en la el Convenio. Pese a que no es preciso que dicha violación se haya producido de forma efectiva, sí se ha venido exigiendo que exista esa «queja defendible» (*arguable complaint*) bajo el Convenio —Sentencia del TEDH (Gran Sala) de 23 de febrero de 2012, caso *Hirsi Jamaa contra Italia*, §197—, que desde una primera aproximación verosímil permita después componer un relato de los hechos fiable, a la vista de que el Convenio tiene por objeto garantizar derechos prácticos y efectivos, no teóricos o ilusorios —Sentencia del TEDH (Gran Sala) de 13 de febrero de 2020, caso *N. T. y N. D. contra España,* §171—. Por ello, es extraño encontrar violaciones aisladas del artículo 13 en las que no se encuentre ninguna otra infracción, aunque doctrinalmente la posibilidad existe, y de hecho se ha producido —Sentencia del TEDH (Gran Sala) de 8 de julio de 2003, caso *Hatton y otros contra Reino Unido*—. Dentro del ámbito del derecho de asilo, esta relación se ha vehiculado casi invariablemente a través de la conexión de la infracción con violaciones del artículo 3 del CEDH[8] y del artículo 4 de su Protocolo número 4[9].

2.2.2.2. Derecho a la no devolución

Por su parte, el derecho a la no devolución (recogido en el artículo 33 de la Convención de Ginebra y habitualmente referido como *non-refoulement,* en la doctrina internacional) se erige como un principio básico de la protección internacional que implica la garantía de que el beneficiario de ésta no será, mientras mantenga su condición, devuelto a su Estado de origen ni a ningún otro en el que corra el riesgo de ser perseguido. Este derecho se extiende de forma directa a los solicitantes durante la instrucción de su expediente y, en el ámbito de la UE, incluso a aquellos que no hayan obtenido oficialmente la protección internacional o les haya sido retirada (art. 14.6 de la Directiva 2011/95/UE), en la medida en que «son las circunstancias de facto de una persona, [y] no la validación oficial

[7] «Toda persona cuyos derechos y libertades reconocidos en el presente Convenio hayan sido violados tiene derecho a la concesión de un recurso efectivo ante una instancia nacional, incluso cuando la violación haya sido cometida por personas que actúen en el ejercicio de sus funciones oficiales».
[8] «Nadie podrá ser sometido a tortura ni a penas o tratos inhumanos o degradantes».
[9] «Quedan prohibidas las expulsiones colectivas de extranjeros».

de esas circunstancias, las que dan lugar al estatus de refugiado de la Convención» (Hathaway, 1995, 303-304). Y, al mismo tiempo, su observancia es independiente de si el solicitante se encuentra en situación legal o no en el país, extremo que —pese a no mencionarse explícitamente en el articulado de la Convención— se ha impuesto por la vía del derecho internacional consuetudinario y, en el caso europeo, se ha normativizado mediante el artículo 19 de la CDFUE y el artículo 9 de la Directiva 2013/32/UE, siendo avalado mediante de una reiterada y pacífica jurisprudencia al respecto en el marco del sistema europeo de protección de los derechos humanos[10]. Ello hace que el derecho a la no devolución se haya configurado como parte del núcleo más esencial de los derechos del refugiado, en la lógica de que su vulneración sistemática supondría, en la práctica, el vaciamiento de contenido de la protección internacional.

Es destacable que este principio admite una excepción: el artículo 33.2 de la Convención de Ginebra avala su inaplicabilidad en aquellos casos en que existan «razones fundadas» para considerar que el beneficiario o solicitante de protección internacional pueda ser considerado «un peligro para la seguridad del país donde se encuentra» (art. 33.2). Esta provisión, que refuerza las prerrogativas de los Estados en el marco de su legítimo derecho a la protección de sus fronteras, ha sido avalada, con ciertos matices[11], por la jurisprudencia internacional. Buena muestra de ello es la sentencia del TEDH (Gran Sala) de 29 de abril de 1997, caso *L. H. R. contra Francia*, en el marco de la cual el tribunal avala la deportación de un nacional colombiano condenado por tráfico de drogas a su país de origen, basándose en que su presencia supone una «seria amenaza para el orden público», todo ello pese a las alertas del demandante —compartidas por la hoy extinta Comisión Europea para los Derechos Humanos, e incluso tibiamente por el propio tribunal— de que la culminación de su expulsión podía suponer un peligro para su vida.

Finalmente, una última cuestión destacable es que el desarrollo del principio de no devolución ha dado lugar, con el paso del tiempo, al surgimiento de un principio complementario que ha sido recogido de forma generalizada por los instrumentos legales internacionales más importantes en la materia: la proscripción de las expulsiones colectivas de extranjeros. Dicho precepto, que algunos autores como Kamto (2007) consideran (no sin polémica) como un «principio general del derecho internacional» (p. 129), ha sido normativizado en el CEDH (artículo 4 del protocolo 4º) y en la CDFUE (artículo 19.1). Su contenido refiere al planteamiento de que toda expulsión de extranjeros debe estar basada en circunstancias no arbitrarias, y por ende se hace necesario que se evalúe el contexto de cada extranjero de forma individual.

---

[10] Sentencias del TEDH de 7 de julio de 1989, caso *Soering contra el Reino Unido* y, especialmente, de 15 de noviembre de 1996, caso *Chahal contra Reino Unido*.

[11] Por ejemplo, la implementación de este precepto en el ámbito europeo no debe suponer que, por omisión, se provoque la vulneración del artículo 3 de la CEDH, que proscribe la tortura y las penas o tratos inhumanos o degradantes; factor que, por otra parte, es aplicable a toda la comunidad internacional, al haberse considerado como un argumento con naturaleza de *ius cogens* (Sentencia del Tribunal Penal Internacional para la antigua Yugoslavia de 22 de febrero de 2001, caso *Fiscalía contra Dragoljub Kunarac Radomir Kovac And Zoran Vukovic*, §466; o Sentencia del Tribunal Internacional de Justicia de 20 de julio de 2012, Cuestiones relativas a la obligación de juzgar o extraditar, *Bélgica contra Senegal*, §99).

ORCID: https://orcid.org/0000-0003-0162-4213

3. ANÁLISIS JURÍDICO: POSTURAS ENFRENTADAS Y RESPUESTA DE LOS TRIBUNALES

3.1. CASO *HIRSI JAMAA CONTRA ITALIA*: LA GÉNESIS DE UNA DOCTRINA

Sobre la base de la legislación expuesta con anterioridad, los sucesivos pronunciamientos judiciales han ido cincelando el marco regulatorio final que, al menos por el momento, rige el complicado equilibrio entre las legítimas potestades estatales y la salvaguarda de los derechos fundamentales. A tal efecto, destaca sobre todas las demás una sentencia que, por el marco temporal en el que fue dictada y sus implicaciones políticas posteriores, ha supuesto una referencia insoslayable a la hora de establecer los criterios mínimos de actuación en frontera: se trata de la Sentencia (Gran Sala) del TEDH de 23 de febrero de 2012, caso *Hirsi Jamaa y otros contra Italia*.

Hirsi Jamaa es el nombre de un ciudadano somalí integrado en un grupo de aproximadamente doscientos inmigrantes clandestinos, los cuales fueron desembarcados, entre el 6 y el 7 de mayo de 2009, en el puerto de Trípoli. Dicho desembarco se produjo directamente desde los tres buques de Estado italianos (*Guardia di Finanza* y Guardacostas) que habían procedido, pocas horas antes, a la interceptación y rescate del grupo mientras navegaba en sendas embarcaciones precarias, a unas 35 millas náuticas al sur de la isla de Lampedusa, en zona de búsqueda y rescate (en adelante SAR, por sus siglas en inglés) maltesa. Con motivo de tales hechos se demandaría a Italia frente al TEDH, contándose un total de veinticinco adheridos a la referida causa.

Sin embargo, lo relevante —por novedoso— de *Hirsi Jamaa* no fue tanto la aplicación del artículo 3 del CEDH en el contexto de un retorno de inmigrantes —praxis ya consolidada en sentencias como *Chahal contra Reino Unido*—, sino que, por primera vez, el tribunal tenía ocasión de pronunciarse sobre un rechazo de inmigrantes interceptados en el medio marítimo al mismo tiempo que se valoraba la aplicación extraterritorial del CEDH (Alarcón Velasco, 2015, p. 4). Y lo hizo asestando un contundente varapalo a las tesis italianas, ya que declaró la violación de los artículos 3 y 13 del CEDH, así como del artículo 4 de su protocolo número 4, en todos los casos por unanimidad.

Los razonamientos nucleares que sustentaron la postura del tribunal fueron los siguientes:

1. A nivel general, el CEDH es aplicable, en tanto en cuanto, conforme a los artículos 92 y 94 de la Convención de las Naciones Unidas sobre el Derecho del Mar, los buques en los que transcurren los hechos se encuentran sometidos a la jurisdicción de su Estado de abanderamiento, tratándose de un caso de «ejercicio extraterritorial de jurisdicción […] susceptible de implicar la responsabilidad del Estado».
2. Respecto del artículo 3, el factor determinante se situó en la imposibilidad de considerar Libia como un «lugar seguro» (en inglés, «*place of safety*») para el desembarco, al valorar el tribunal que no solo debía tenerse en cuenta la seguridad

desde el punto de vista marítimo[12], sino también las cuestiones relativas a la protección de sus derechos fundamentales (ruptura del principio de no devolución).

3. Respecto del artículo 4 del protocolo 4, el factor determinante se situó en la no individualización de la expulsión de los inmigrantes, en tanto en cuanto no se les identificó ni se valoró si alguno de ellos podía contar con circunstancias personales relevantes (violación de la prohibición de las expulsiones colectivas).

4. Respecto del artículo 13, el factor determinante se situó en la imposibilidad de los inmigrantes de acceder a un recurso efectivo frente a la decisión de la expulsión (infracción del derecho a la tutela judicial efectiva), factor valorable al haberse constatado la vulneración del artículo 3.

3.2. CASO *N. D. Y N. T. CONTRA ESPAÑA*: LOS LÍMITES A LA PROTECCIÓN

Tal y como se ha tenido ocasión de exponer en los epígrafes anteriores, la universalidad del derecho a solicitar protección internacional no implica que tal derecho pueda reclamarse o ejercerse de manera ilimitada. La Sentencia del TEDH (Gran Sala) de 13 de febrero de 2020, en el marco del caso *N. D. y N. T. contra España*, no será sino uno de los mejores ejemplos de cómo las naciones pueden, por sí mismas, establecer esquemas eficientes de control fronterizo que, a su vez, sean respetuosos con el derecho internacional humanitario, combatiendo el abuso de derecho desde una perspectiva garantista.

Emulando el análisis efectuado durante el epígrafe anterior respecto de *Hirsi Jamaa*, en el presente caso se tiene a dos ciudadanos extranjeros N. D. y N. T., los cuales, formando parte de un grupo integrado por unas 600 personas, intentan asaltar el vallado fronterizo existente en la ciudad de Melilla a primera hora del día 13 de agosto de 2014. Frustrado su intento gracias a la acción de la Guardia Civil y las fuerzas de seguridad marroquíes, los dos demandantes fueron escoltados al otro lado de la frontera, acto que motivará la demanda. Posteriormente, ambos actores participarían en dos nuevos asaltos al vallado, logrando acceder ilegalmente a territorio español. Es relevante el hecho de que uno de ellos llegará a solicitar protección internacional con posterioridad, si bien ésta se le es denegada en todas las instancias procesales.

Llegados a este punto, el interés de la sentencia es doble. Por un lado, porque supuso el aval definitivo a la práctica del «*rechazo en frontera*» (peyorativamente referida en ocasiones como «*devolución en caliente*»): la ejecución de un retorno inmediato a Marruecos de todo inmigrante sorprendido mientras intenta superar ilegalmente los elementos de contención fronterizos. Y, por otro, porque supone un contrapunto con respecto a *Hirsi Jamaa*, ya que ambas marcan los límites de la legalidad desde un prisma diferente: positivo en *N. D. y N. T.* (aquello que sí se puede hacer), negativo en *Hirsi Jamaa* (aquello que no se puede hacer), señalando así las dos lindes entre las cuales debe discurrir la legislación fronteriza. Todo ello en el contexto que supone la existencia, en este caso, de

[12] La ausencia de riesgo de los conceptos relacionados con la seguridad en el mar que pueden encontrarse en los convenios internacionales en la materia (especialmente en los convenios SAR y SOLAS) alude mayoritariamente, por referencia, a aspectos relacionados con la seguridad de la navegación u operativa (*safety*, seguridad como protección frente al naufragio, frente al ahogamiento, frente a los riesgos inherentes a la carga del buque, etc.). No obstante lo anterior, y en relación con el concepto de «*place of* safety» existente en el convenio SAR de 1979, la propia Organización Marítima Internacional (en adelante IMO, por sus siglas en inglés) ha acabado por integrar matices que complementen dicha visión, dando como resultado textos como el anexo 34 de la resolución IMO MSC.167(78), *Guidelines on the treatment of persons rescued at sea*, en el que se hace referencia a regulaciones como la Convención de Ginebra de 1951.

ORCID: https://orcid.org/0000-0003-0162-4213

un pronunciamiento de instancia que contrariaba las tesis de España, lo que da lugar a un proceso de fundamentación más detallado por la Gran Sala frente a las demandas de los actores, que promovían la impugnación de la actuación de los guardias de fronteras por violación del artículo 3 del CEDH y del artículo 4 del protocolo 4 del CEDH, así como del artículo 13 del CEDH en relación con los dos anteriores.

Así pues, se tiene que los razonamientos nucleares que sustentaron la postura del tribunal fueron los siguientes:

1. Respecto del artículo 3, ya en la misma fase de admisión (decisión de 7 de julio de 2015), el tribunal rechaza de plano la admisibilidad de las tesis de los demandantes en cuanto a la posibilidad de que se hubiera incumplido el principio de no devolución (artículo 3 CEDH) por el rechazo de los inmigrantes de vuelta a Marruecos. Si bien el razonamiento jurídico no es especialmente detallado, sí reseña palmariamente la ausencia de indicios para considerar a Marruecos un lugar inseguro a tales efectos, y ni siquiera —como sí que hizo en el caso de Hirsi Jamaa— considera necesario plantear un estudio más profundo de la cuestión.
2. Respecto del artículo 4 del protocolo 4, la tesis del tribunal establece que no puede considerarse la existencia de una expulsión colectiva en el marco de una actuación en fuerza desencadenada por el propio demandante, y que provoca «una situación claramente perturbadora, difícil de controlar y que pone en peligro la seguridad pública» (§201). Esto es especialmente relevante si tenemos en cuenta que, en la sentencia de instancia, la Sala había establecido de forma directa —sin tan siquiera plantear una justificación que incidiera en el fondo del asunto— un paralelismo total de este caso con Hirsi Jamaa, pese a tratarse de contextos totalmente distintos. Así, la corte dispone que ese «examen individualizado» que permita superar el obstáculo conceptual de la expulsión colectiva, debe efectuarse teniendo en cuenta «las circunstancias particulares de la expulsión y el "contexto general en el momento de los hechos"» (§197), lo que a su vez permite que los trámites de evaluación puedan simplificarse o directamente omitirse, especialmente si dicho contexto depende mayoritariamente «de la propia conducta del demandante» (§200) y si por parte del Estado se ofrecen «procedimientos legales disponibles para entrar [al país]» (§208) y «se garantiza el derecho a solicitar protección […] de forma real y eficaz» (§208).
3. Respecto del artículo 13, el tribunal clarifica que no puede hallarse vulneración del derecho a la tutela judicial efectiva, achacando también la falta del recurso judicial a «la propia conducta de los demandantes al intentar entrar sin autorización en Melilla» (§242).

Finalmente, una apreciación interesante sobre la fundamentación de la sentencia es que, al tiempo que el tribunal rechaza las tesis de España en lo relativo a la limitación de la jurisdicción en base a criterios operativos —similares a las sostenidas por Italia en *Hirsi Jamaa*—, afirmando que resulta innegable el ejercicio efectivo de autoridad que España, a través de la Guardia Civil ejerce desde el perímetro de la alambrada exterior hacia adentro (§§107-108), establece que no puede hacerse responsable al Gobierno español de circunstancias que se producen fuera de su territorio soberano, y en particular de aquellas desempeñadas por agentes de un Estado tercero (§218).

3.3. ANÁLISIS COMPARATIVO: LA COMPATIBILIZACIÓN DE UNA DOCTRINA JURISPRUDENCIAL DISPAR

Como hemos visto, tanto *Hirsi Jamaa y otros contra Italia* como *N. D. y N. T. contra España* suponen dos casos en los que, para conductas a priori análogas (la entrega a autoridades no europeas de extranjeros que intentan acceder ilegalmente a territorio comunitario) el TEDH ha ofrecido resoluciones diferentes. Y esto se debe, fundamentalmente, a la existencia en el caso *N. D. y N. T.* de un hilo conductor que fue oportuna y debidamente reivindicado por España en el marco del proceso seguido durante el referido contencioso, y que articula, de principio a fin, la sentencia: la doctrina de la «conducta culpable».

El corolario de este razonamiento se concreta en que no puede imputarse al Estado la responsabilidad de que los inmigrantes eludan los procedimientos legales para acceder al país, especialmente si estos «se aprovechan deliberadamente de su gran número y utilizan la fuerza» (*N. D. y N. T. contra España*, §201). Así, para que dicha doctrina resulte aplicable, la conducta reprochable atribuible a los inmigrantes debe generar una situación grave, derivada de un comportamiento doloso —es decir, consciente de su ilegalidad y de sus posibles consecuencias— que represente un peligro objetivo para la seguridad pública, incluida la de los propios inmigrantes.

Y es que, ciertamente, la interpretación del tribunal trasciende a todas las presuntas contravenciones alegadas por los demandantes, incluso a aquellas que (a priori) se encuentran más alejadas de su esfera de actuación individual. Así, al respecto de la proscripción de las expulsiones colectivas de extranjeros (artículo 4 del protocolo 4º del CEDH), el TEDH situará el aspecto diferencial en las posibilidades de acceso, por parte de los inmigrantes, a procedimientos legales de entrada en el territorio europeo. Así, en *N. D. y N. T.*, se reseña en repetidas ocasiones que la legislación española ofrecía diversas posibilidades para que los demandantes tramitaran su entrada en España, así como para que solicitaran asilo[13] (§212), pero que por parte de estos se rehusaron (conducta culpable) tales herramientas (§231). Análogo razonamiento resulta aplicable al respecto del derecho a la tutela judicial efectiva (artículo 13 del CEDH), por ser los mismos los argumentos empleados por la corte de garantías (§242).

Una vez expuestas estas premisas, la pregunta se hace inevitable: ¿Cabría emplear, *mutatis mutandis*, la doctrina de la conducta culpable para expulsiones que tuvieran lugar en el ámbito marítimo? Y, de ser así, ¿Qué sería necesario cambiar en el marco de la actuación de los Estados para ello? La respuesta a estas preguntas no es trivial. Tras *N.*

[13] Resulta especialmente destacable la posibilidad que ofrece la legislación española de acceder a determinados procedimientos relacionados con el asilo en embajadas y consulados (artículo 38 de la Ley 12/2009, de 30 de octubre, reguladora del derecho de asilo y de la protección subsidiaria), tanto por la reiteración con la que el tribunal se afana en señalar esta posibilidad como por no ser una práctica común en otros Estados europeos (Italia, sin ir más lejos, no lo recoge en su Decreto Legislativo de 19 noviembre de 2007, de reconocimiento de protección internacional).

ORCID: https://orcid.org/0000-0003-0162-4213

D. y N. T., el TEDH ha empleado esta doctrina —que, por otra parte, tampoco era totalmente nueva en el momento de su formulación[14]— en contadas ocasiones[15], si bien ninguna de ellas ha servido para avalar un rechazo marítimo. Sin embargo, lo cierto es que no existe ningún pasaje de *N. D. y N. T.* en el que el tribunal advierta que su doctrina no es válida para expulsiones de inmigrantes interceptados en el mar. Más bien al contrario: la sentencia incide en la necesidad de la evaluación de las «circunstancias del caso concreto» (§201). A resultas de esto, y bajo el principio *permissum videtur id omne quod non prohibitur*[16], parece lógico deducir que la admisibilidad de tal principio debería depender únicamente del cumplimiento de sus presupuestos intrínsecos; esto es, de la existencia de herramientas legales reales que permitan acceder al Estado de destino y de impulsar un procedimiento asilo ante sus autoridades; así como de la constatación de una conducta reprochable por parte de los inmigrantes que, al tiempo que desprecie la existencia de tales herramientas legales, desafíe los mecanismos de control fronterizo mediante una acción coactiva. Asimismo, ambos presupuestos deben ser debidamente alegados por el Estado en el marco del proceso judicial, algo que Italia no hizo en *Hirsi Jamaa*. Ninguno de estos requisitos previos parece necesariamente invencible en un escenario marítimo tipo, según el cual centenares de varones de origen y antecedentes desconocidos se pongan a sí mismos, a sus compañeros de viaje y a los guardias europeos de fronteras y costas en un peligro manifiesto, mediante el planteamiento de una salida masiva, planificada y coordinada de embarcaciones con rumbo a un territorio aislado, el cual adolezca de unas capacidades de acogida limitadas, con el consiguiente riesgo de colapso —como puede ser el de Lampedusa—. Todo ello salvando la necesidad de que por parte del Estado ribereño se cuente con un despliegue diplomático adecuadamente dimensionado y con facultades concedidas en el ámbito del asilo, el cual permita justificar la suficiencia de mecanismos de acceso al mismo. A este respecto, cabe mencionar también la comunidad que en materia de migración y asilo supone la UE, lo que incluso permitiría plantear —aunque quizás para ello sería necesario avanzar algo más en la siempre pausada integración europea— que la existencia de delegaciones diplomáticas de otros países de la Unión es un activo que necesariamente debe ser valorado a los efectos de ponderar adecuadamente las posibilidades de acceso que ofrece el Estado litigante, por suponer un refuerzo consustancial a los medios del propio Estado[17].

Y, al hilo de lo anterior, es también pertinente traer a colación determinadas inferencias al respecto del problema de las limitaciones fácticas del Estado en su acción internacional. Y es que, pese a que determinados autores como Sánchez Tomás (2018, p.

---

[14] Ya en 1996 el TEDH había utilizado un enfoque precursor de este en el caso *John Murray contra Reino Unido* —Sentencia (Gran Sala) de 8 de febrero de 1996—, al denegar el amparo a un condenado por terrorismo que alegaba que se había utilizado su silencio contra él en el marco de su proceso judicial. El tribunal resolvió que había sido él quien había elegido guardar silencio pese a conocer las consecuencias que tal conducta podía implicar, y que por tanto fue él quien se expuso a que de ese silencio se infirieran extremos que le perjudicaban (§56).

[15] Sentencia del TEDH (Sección Tercera) de 24 de marzo de 2020, caso *Asady y otros contra Eslovaquia.*

[16] «Se considera permitido todo lo no prohibido».

[17] Al fin y al cabo, parece evidente pensar que, al preexistir un espacio común de libertad, seguridad y justicia, en el marco del cual se han abolido las fronteras interiores y que ha articulado mecanismos para ejecutar una política común de inmigración y asilo, una red compuesta por todas y cada una de sus embajadas y consulados supone para los candidatos a la inmigración una plataforma de acceso mucho mayor, más diversificada y con una mayor cantidad de garantías procedimentales que la que ofrece un Estado por separado. Especialmente si tenemos en cuenta la homogeneidad que implica la legislación europea con respecto al reconocimiento, cualificación, evaluación y resolución de procedimientos de asilo, estancia y residencia legal, que son comunes para todos los Estados que la componen.

110) o Martínez Escamilla (2021, pp. 6-7) reivindiquen la territorialidad como perspectiva dominante en cuanto a la determinación de la responsabilidad internacional, lo cierto es que tanto la doctrina como la práctica internacional (ya referidas en el punto 2.1.2 de este texto) apuntan hacia la necesidad de un ejercicio práctico de la autoridad en dicho territorio para poder considerarlo soberano, razón por la cual el tribunal, en su sentencia de Gran Sala, enmienda su pronunciamiento de instancia al eliminar o suavizar enormemente las menciones relativas a la preponderancia del trazado de la frontera frente al recorrido real del vallado (incluidas en el §53 de la sentencia de instancia). Así, como ya hemos referido, el rechazo de la exención del principio general de atribución no pivota en torno a la territorialidad del punto donde suceden los hechos, sino a que la actuación es desarrollada por agentes del Estado signatario, independientemente de donde se efectúe la acción. Esto será relevante en casos (por ejemplo, los hechos ocurridos el 24 de junio de 2022 en Melilla) en los que se ha pretendido hacer responsable a España de hechos llevados a cabo por funcionarios extranjeros en espacios que, aunque formalmente se pudieran encontrar dentro del trazado fronterizo «histórico» español, en la práctica se hallen situados más allá del vallado, y por ende no se ejerce control efectivo sobre ellos por parte de España.

Para finalizar, debemos reseñar el distinto trato que el tribunal dispensa al estudio de las posibles vulneraciones del artículo 3 CEDH (prevención de la tortura y los tratos inhumanos o degradantes) en *Hirsi Jamaa* y en *N. D. y N. T.* Pese a la escasa fundamentación que ofrece la decisión de inadmisión de *N. D. y N. T.* a ese respecto, parece evidente que la justificación de tal diferencia reside, al menos en su mayor parte, en el país de expulsión. Y es que parte de la doctrina (Del Valle Gálvez, 2018, pp. 25-49; Freedman, 2024, 204-220) ha llegado a plantear tesis que se acercan a un cuestionamiento generalizado de lo que se ha venido a llamar «políticas de externalización de fronteras», concepto con el que es preciso ser muy cautos. En primer lugar, porque mediante ese término peyorativo se han definido lo que no son más que, en la mayoría de los casos, políticas de cooperación policial internacional en materia de control fronterizo, a través de las cuales se fomenta la creación de capacidades para reforzar la garantía del cumplimiento de la ley en cuerpos de seguridad en países en vías de desarrollo. Así pues, incluso el propio término escogido parece bastante poco afortunado, ya que difícilmente pueden «externalizarse» unas tareas, las de control fronterizo y aplicación de la ley, que no son sino «obligaciones derivadas tanto del derecho convencional como consuetudinario», y por tanto, objeto de «*ius cogens*» (Soler García, 2017, p. 41). Y, por otro lado, porque aceptar de forma irracional posturas tangencialmente contrarias a estas políticas pondría en peligro no solo la aplicación de medidas legítimas del Estado —expresión de su soberanía en materia de seguridad nacional o política migratoria—, sino también los intereses de la comunidad internacional y la protección de los derechos humanos: al fin y al cabo, la construcción de capacidades de los Estados de origen y tránsito en cuestiones vitales como la búsqueda y rescate en el mar de sus propios compatriotas es también parte esencial de esta cooperación. De ello se deduce que tal cooperación *per se* no puede contradecir el CEDH.

Y es ahí donde entra el factor verdaderamente diferencial en *Hirsi* Jamaa: Libia. En tal sentido, lo cierto la situación de Libia es idiosincrática. Se trata de un Estado que no ha suscrito la Convención de Ginebra, el cual ha sido reiteradamente definido por distintos autores como un «caos», en el cual «los inmigrantes expulsados desde Europa solían quedar abandonados a un destino incierto» (Cole, 2012, p. 6). Y ello explica a la perfección los temores expresados por el tribunal en *Hirsi Jamaa* (§136), sobre la base de

ORCID: https://orcid.org/0000-0003-0162-4213

distintos informes incorporados a la causa (ACNUR, Comisión Europea, Consejo de Europa, Human Rights Watch, etc., v. §33-42). Esta situación no es comparable con la existente en la práctica totalidad de los Estados con los que España mantiene acuerdos activos y razonablemente funcionales de repatriación, principalmente Marruecos y Argelia, Estados integrados en la Política Europea de Vecindad —la cual exige, conforme al artículo 8 del TUE, compartir los principios democráticos de la UE— y que se han beneficiado en gran medida de ello, convirtiéndose en socios económicos y políticos privilegiados. Al fin y al cabo, existe una gran cantidad de pronunciamientos judiciales[18] que avalan explícitamente su carácter de «terceros países seguros» (véanse la SAN 1441/2018, de 15 de marzo de 2018 para el caso de Marruecos o la SAN 3838/2016, de 17 de octubre de 2016 para el caso de Argelia). Y este es un punto de gran interés no solo a efectos del retorno de inmigrantes en situación irregular a sus países de origen, sino también en relación con la posibilidad (avalada por el artículo 3.3 del Reglamento 604/2013 sobre la determinación del Estado miembro responsable del examen de una solicitud de protección internacional) de remitir a los solicitantes de asilo a centros localizados en terceros países seguros durante la revisión de su solicitud. Sin embargo, esta posibilidad podría ser objeto —dada su complejidad y su previsible polémica— de un artículo completo aparte, con su correspondiente debate doctrinal.

4. CONCLUSIONES

Para concluir, realizaremos una breve síntesis de la doctrina revisada en los capítulos anteriores, ofreciendo unas líneas maestras que describan los hallazgos de mayor interés en la materia objeto de análisis.

En primer lugar, la conclusión de carácter más general y evidente que puede extraerse de todo cuanto antecede es que en el entorno fronterizo confluyen numerosos fenómenos sociales, los cuales generan una elevada litigiosidad en torno a la tutela de los derechos fundamentales. Estos procesos, derivados todos ellos de la permanente tensión entre las políticas de control migratorio y las garantías individuales, exigen un equilibrio que a menudo se dirime en los tribunales, poniendo a prueba los marcos jurídicos nacionales e internacionales; así como una serie de conceptos manejados por la doctrina —frontera, soberanía, territorio, asilo, etc.— los cuales, pese a ser empleados habitualmente de forma trivial, poseen un contenido de gran potencia jurídica, política, social e incluso histórica. Por ello, es fundamental que por parte de las fuerzas de seguridad que prestan su servicio en frontera exista un conocimiento suficiente de la legislación que les ampara, a fin de desarrollar sus cometidos de forma eficiente, pero también respetuosa con los derechos de aquellos que transiten tales entornos.

Por otro lado, es destacable que la mayor parte de esos procesos judiciales se sustancian en relación con la vulneración de unas garantías muy concretas, las cuales se repiten de forma habitual en los pronunciamientos de los órganos judiciales que se encargan

[18] La práctica totalidad de estos pronunciamientos provienen de los ámbitos nacionales, toda vez que el TEDH evita pronunciamientos categóricos al respecto de la seguridad de los Estados y prioriza el análisis caso por caso, al igual que los altos tribunales españoles. Por otra parte, Varios países europeos han elaborado listas de terceros países seguros, incluyendo a Marruecos en algunas de ellas, como ocurre, por ejemplo, en los Países Bajos (Servicio de Inmigración y Naturalización, 2018). Esta práctica está ganando terreno entre los Estados europeos y se alinea con lo establecido en el Pacto de Migración y Asilo, que ha introducido dicho concepto en el nuevo Reglamento de Procedimientos de Asilo (Reglamento (UE) 2024/1348), que comenzará su aplicación a partir del 12 de junio de 2026 (Sección V, arts. 57 y ss.).

de su enjuiciamiento. Se trata fundamentalmente de la transgresión de los principios de no devolución y del derecho a la tutela judicial efectiva, doctrinas cuya salvaguarda, en el marco europeo, se incardina en los artículos 3 y 13 del CEDH; así como de la prohibición de las expulsiones colectivas de extranjeros, amparada en el artículo 4 del protocolo 4º de dicho Convenio. Estos procesos judiciales, no obstante, son largos, muy complejos y en no pocas ocasiones sus resoluciones entran en conflicto directo con pronunciamientos anteriores de otros tribunales o incluso de los mismos órganos que los emiten. Por tales razones, es también preceptivo que los organismos encargados de la representación y defensa de los Estados soberanos tengan un conocimiento profundo del Derecho Internacional, y sepan compatibilizar tales doctrinas con su derecho interno —proponiendo incluso las modificaciones legislativas que sean necesarias—; todo ello con el objeto de asegurar, como garantes que también son del ordenamiento jurídico, que los pronunciamientos que afecten a sus ámbitos de representación se encuentren alineados con la ley y la práctica internacional.

En último término, y en línea con todo lo anterior, no puede pasarse por alto la mutabilidad que caracteriza la interpretación del ordenamiento jurídico internacional. Esto no es una debilidad del sistema en sí misma: Las normas, especialmente en entornos anárquicos como este, se encuentran en un permanente proceso de transformación, y por ello los operadores jurídicos no tienen más remedio que adaptar sus posturas a las realidades existentes, algo que lleva haciéndose desde una antigüedad en la que existían figuras jurídicas impensables en el mundo contemporáneo. En tal sentido, un escenario tan volátil como el que rige la geopolítica mundial actual exige —dentro del respeto a los consensos inherentes al mantenimiento de la paz y seguridad internacional, entre los que se encuentra la consideración de la dignidad de la persona como fuente inalienable de los derechos humanos— un cierto margen en la interpretación de las normas que presiden las obligaciones de los Estados, postura que no es nueva en la doctrina (Koskenniemi, 2004). De esta forma, se garantiza un adecuado cumplimiento de aquellas, respetándose la voluntad de sus impulsores al tiempo que se favorece la convivencia, profundizándose así en el desarrollo de un entorno internacional próspero para todos sus habitantes.

REFERENCIAS BIBLIOGRÁFICAS

Alarcón Velasco, N. (2015), El abogado ante las normas de asilo: vigilancia de su aplicación, Consejo General de la Abogacía Española. Disponible en línea: https://www.abogacia.es/actualidad/noticias/el-abogado-ante-las-normas-de-asilo-vigilancia-de-su-aplicacion/. [Fecha de la consulta: 31/03/2025].

Carrasco Durán, M. (2020). La definición constitucional del derecho a la tutela judicial efectiva, en Revista de derecho político, núm. 107, 13-40.

Cole, P. (2012), Borderline Chaos? Stabilizing Libya's Periphery, Middle East, Octubre de 2012, Washington: Carnegie Endowment for International Peace.

Comisión Española de Ayuda al Refugiado (3 de octubre de 2017), El Tribunal Europeo de DDHH condena a España por dos 'devoluciones en caliente'. Disponible en línea: https://www.cear.es/noticias/tribunal-europeo-ddhh-condena-espana-dos-devoluciones-caliente-nuestra-frontera-sur/. [Fecha de la consulta: 31/03/2025].

Comisión Europea (2022), Informe sobre el estado de Schengen 2022, Comunicación de la Comisión al Parlamento Europeo, al Consejo Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones, COM(2022) 301 final. Disponible en línea: https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:52022DC0301. [Fecha de la consulta: 31/03/2025].

Comisión Europea (2024), Standard Eurobarometer. Europeans' opinions about the European Union's priorities, núm. 102, Bruselas: Publications Office of the EU. Disponible en línea: https://europa.eu/eurobarometer/surveys/detail/3215. [Fecha de la consulta: 31/03/2025].

Consejo de la Unión Europea (2015), Council Conclusions on the Middle East Peace Process. Disponible en línea: https://www.consilium.europa.eu/en/press/press-releases/2015/07/20/fac-mepp-conclusions/pdf/. [Fecha de la consulta: 31/03/2025].

Consejo General de la Abogacía Española (3 de octubre de 2017), La Abogacía reitera la ilegalidad de las devoluciones en caliente, tras la condena del TEDH. Disponible en línea: https://www.cear.es/noticias/tribunal-europeo-ddhh-condena-espana-dos-devoluciones-caliente-nuestra-frontera-sur/. [Fecha de la consulta: 31/03/2025].

Curzon, G. (1907), Frontiers, Oxford: Clarendon Press.

Del Valle Gálvez, A. (2019), La fragilidad de los derechos humanos en las fronteras exteriores europeas, y la externalización/ extraterritorialidad de loscontroles migratorios en Anuario de los cursos de derechos humanos de Donostia-San Sebastián, Vol. XVIII, Valencia: Tirant lo Blanch.

Doebbler, C. (2018), Dictionary of Public International Law, Londres: Row-man & Littlefield.

Eurostat (2025), Population on 1 January by age group, sex and citizenship. Disponible en línea: https://ec.europa.eu/eurostat/databrowser/view/migr_pop1ctz/default/table?lang=en. [Fecha de la consulta: 31/03/2025].

Freedman, J. (2024), The violent externalisation of asylum en Research Handbook on Asylum and Refugee Policy, pp. 204-220, Cheltenham: Edward Elgar Publishing.

Frontex (2021), Risk Analysis for 2021, Varsovia. Disponible en línea: https://www.frontex.europa.eu/publications/risk-analysis-for-2021-MmzGl0. [Fecha de la consulta: 31/03/2025].

Frontex (2024), Annual Brief 2023, Varsovia. Disponible en línea: https://prd.frontex.europa.eu/document/annual-brief-2023/. [Fecha de la consulta: 31/03/2025].

Golmayo, P. B. (1866), Instituciones de Derecho Canónico, Madrid: Imprenta de A. Peñuelas.

Harris Díez, R. (2011), El paisaje de los dioses: los santuarios griegos de la época clásica y su entorno natural, en AISTHESIS: Revista Chilena de Investigaciones Estéticas, núm. 49, Santiago de Chile: Instituto de Estética de la Pontificia Universidad Católica de Chile.

Hathaway, J. C. (2005), The rights of refugees under International Law, Cambridge: Cambridge University Press.

Infante Caffi, M.T. (2016), Las fronteras desde la perspectiva del Derecho Internacional, en Revista de Estudios Internacionales, núm. 185, pp. 59-86, Santiago: Instituto de Estudios Internacionales de la Universidad de Chile. Disponible en línea: https://www.scielo.cl/scielo.php?script=sci_arttext&pid=S0719-37692016000300004. [Fecha de la consulta: 31/03/2025].

Kamto, M. (2007), Third report on the expulsion of aliens, Ginebra: Comisión de Derecho Internacional de las Naciones Unidas.

Koskenniemi, M. (2004), The Gentle Civilizer of Nations: The Rise and Fall of International Law 1870–1960, Cambridge: Cambridge University Press.

Lacan, J. (1966), Écrits, París: Éditions du Seuil.

Martínez Escamilla, M. (2021), Las "devoluciones en caliente" en el asunto N. D. y N.T. contra España (Sentencia de la Gran Sala TEDH de 13 de febrero de 2020) en Revista Española de Derecho Europeo, Núm. 77.

Oficina del Alto Comisionado de Derechos Humanos (2018), Principios y directrices recomendados sobre los derechos humanos en las fronteras internacionales, Ginebra: UNHCR. Disponible en línea: https://acnudh.org/principios-y-directrices-recomendados-sobre-los-derechos-humanos-en-las-fronteras-internacionales/. [Fecha de la consulta: 31/03/2025].

Parlamento Europeo (2015), Resolución del Parlamento Europeo sobre el papel de la UE en el proceso de paz en Oriente Medio. Disponible en línea: https://www.europarl.europa.eu/doceo/document/TA-8-2015-0318_EN.html. [Fecha de la consulta: 31/03/2025].

Real Academia Española (2014), Diccionario de la lengua española (23ª Edición).

Real Academia Española, Diccionario panhispánico del español jurídico (DPEJ). Disponible en línea: https://dpej.rae.es/. [Fecha de la consulta: 31/03/2025].

RTVE (3 de octubre de 2017), El Tribunal Europeo de Derechos Humanos condena a España por dos "devoluciones en caliente" en Melilla. Disponible en línea: https://www.rtve.es/noticias/20171003/tribunal-europeo-derechos-humanos-condena-a-espana-por-dos-devoluciones-caliente-melilla/1625420.shtml. [Fecha de la consulta: 31/03/2025].

Sánchez Tomás, J. M. (2018), Las «devoluciones en caliente» en el Tribunal Europeo de Derechos Humanos (STEDH, As. N.D. Y N.T. vs España, de 03.10.2017), en Revista Española de Derecho Europeo, núm 65, pp. 102-135.

Sanz Donaire, J. J. (2023). Del concepto de frontera, en Boletín de la Real Sociedad Geográfica, Número extraordinario 2023, pp. 253-262. https://doi.org/10.22201/ceiich.24485691e.2014.12.49710.

Servicio de Inmigración y Naturalización (2018), Beoordeling veilige derde landen – Marokko, Informatiebericht SUA IB 2018/105. Disponible en línea: https://puc.overheid.nl/ind/doc/PUC_9890080000_1/1?solrID=PUC_9890080000_1_1&solrQ=morocco. [Fecha de la consulta: 31/03/2025].

Soler García, C. (2017), La Guardia Europea de Fronteras y Costas: ¿Un avance respecto a Frontex? Una valoración provisional, en Revista Electrónica de Estudios Internacionales, núm. 34. Disponible en línea: https://www.reei.org/ index.php/revista/num34/articulos/guardia-europea-fronteras-costas-avance-respecto-frontex-una-valoracion-provisional. [Fecha de la consulta: 31/03/2025].

Zaidman, L. B., Schmitt-Pantel, P. (2002), La religión griega en la polis de la época clásica (Díez Platas Trad.), Colmenar Viejo: Akal.

NORMATIVA Y JURISPRUDENCIA

Carta de las Naciones Unidas (1945), Conferencia de las Naciones Unidas sobre Organización Internacional, firmada en San Francisco el 26 de junio de 1945.

Convención sobre Derechos y Deberes de los Estados (1933), Séptima Conferencia Internacional Americana de Montevideo, Serie Tratados de la Liga de Naciones, volumen 165, página 19.

Convención sobre el Estatuto de los Refugiados (1951), Conferencia de Plenipotenciarios de las Naciones Unidas sobre el estatuto de los refugiados y de los apátridas, firmada en Ginebra el 28 de julio de 1951, Serie Tratados de las Naciones Unidas, Volumen 189, página 137.

Convenio para la Protección de los Derechos Humanos y de las Libertades Fundamentales (1950), hecho en Roma el 4 de noviembre de 1950.

Protocolo sobre el Estatuto de los Refugiados (1967), firmado en Nueva York el 31 de enero de 1967, Serie Tratados de Naciones Unidas número 8791, Vol. 606, p. 267.

Decreto legislativo del 19 novembre 2007, n. 251, Attuazione della direttiva 2004/83/CE recante norme minime sull'attribuzione, a cittadini di Paesi terzi o apolidi, della qualifica del rifugiato o di persona altrimenti bisognosa di protezione internazionale, nonchè norme minime sul contenuto della protezione riconosciuta.

Directiva 2011/95/UE, del Parlamento Europeo y del Consejo, de 13 de diciembre de 2011, por la que se establecen normas relativas a los requisitos para el reconocimiento de nacionales de terceros países o apátridas como beneficiarios de protección internacional.

Directiva 2013/32/UE del Parlamento Europeo y del Consejo, de 26 de junio de 2013, sobre procedimientos comunes para la concesión o la retirada de la protección internacional.

Directiva 2013/33/UE del Parlamento Europeo y del Consejo, de 26 de junio de 2013, por la que se aprueban normas para la acogida de los solicitantes de protección internacional.

Ley 12/2009, de 30 de octubre, reguladora del derecho de asilo y de la protección subsidiaria.

Reglamento (UE) n ° 604/2013 del Parlamento Europeo y del Consejo, de 26 de junio de 2013, por el que se establecen los criterios y mecanismos de determinación del Estado miembro responsable del examen de una solicitud de protección internacional presentada en uno de los Estados miembros por un nacional de un tercer país o un apátrida.

Reglamento (UE) 2024/1348 del Parlamento Europeo y del Consejo, de 14 de mayo de 2024, por el que se establece un procedimiento común en materia de protección internacional en la Unión y se deroga la Directiva 2013/32/UE.

Tribunal Europeo de los Derechos Humanos (1997), case of H. L. R. v. France, Sentencia (Gran Sala) de 29 de abril de 1997.

Tribunal Europeo de los Derechos Humanos (2012), caso Hirsi Jamaa y otros contra Italia Sentencia (Gran Sala) de 23 de febrero de 2012.

Tribunal Europeo de los Derechos Humanos (2015), caso N. D. y N. T. contra España, Decisión (Sección Tercera) de 7 de julio de 2015.

Tribunal Europeo de los Derechos Humanos (2017), caso N. D. y N. T. contra España, Sentencia (Sección Tercera) de 3 de octubre de 2017.

Tribunal Europeo de los Derechos Humanos (2020), caso N. D. y N. T. contra España, Sentencia (Gran Sala) de 13 de febrero de 2020.

Tribunal Permanente de Justicia Internacional (1933), Legal status of Eastern Greenland, Sentencia de 5 de abril, Series A./B., Fascículo núm. 53, Leiden: A. W. Sijthoff's Publishing Company.

Tribunal Internacional de Justicia (2002), Affaire relative à la souveraineté sur Pulau Ligitan et Pulau Sipadan, Sentencia de 17 de diciembre, nº de vente 858.

Tribunal Internacional de Justicia (2012), Questions relating to the Obligation to Prosecute or Extradite (Belgium v. Senegal), Sentencia de 20 de julio de 2012,

Tribunal Permanente de Arbitraje De La Haya (1998), Territorial Sovereignty and Scope of the Dispute (Eritrea and Yemen), Laudo de 9 de octubre, en Reports of International Arbitral Awards, volumen XXII pp. 209-332.

Tribunal Penal Internacional para la antigua Yugoslavia (2001), Prosecutor v. Dragoljub Kunarac Radomir Kovac and Zoran Vukovic, Sentencia de 22 de febrero de 2001.

Audiencia Nacional (2018), Sentencia 1441/2018, de 15 de marzo de 2018.

Revista Científica del Centro Universitario de la Guardia Civil
Revista Logos Guardia Civil

Artículo de Investigación

LA GUERRA DE NIXON CONTRA LAS DROGAS Y EL AUGE DE LA VIGILANCIA FRONTERIZA VIRTUAL EN ESTADOS UNIDOS

Traducción al Español con la ayuda de IA (DeepL)

J. Luigi M. Kunz Saponaro
Investigador doctoral en la Universidad Carlos III de Madrid.
Máster en Geopolítica y Estudios Estratégicos.
Máster en Seguridad, Defensa y Geoestrategia.
jkunz@hum.uc3m.es

Recibido 31/03/2025
Aceptado 21/05/2025
Publicado 27/06/2025

Cita recomendada: Kunz Saponaro, J. L. M. (2025). La guerra de Nixon contra las drogas y el auge de la vigilancia fronteriza virtual en Estados Unidos. *Revista Logos Guardia Civil*, 3(2), p.p. 147-170.

Licencia: Este artículo se publica bajo la licencia Creative Commons Atribución-NoComercial-SinDerivadas 4.0 Internacional (CC BY-NC-ND 4.0)

Depósito Legal: M-3619-2023
NIPO en línea: 126-23-019-8
ISSN en línea: 2952-394X

LA GUERRA DE NIXON CONTRA LAS DROGAS Y EL AUGE DE LA VIGILANCIA FRONTERIZA VIRTUAL EN ESTADOS UNIDOS

Sumario: 1. INTRODUCCIÓN. 2. REVISIÓN BIBLIOGRÁFICA SOBRE FRONTERAS Y VIGILANCIA VIRTUAL. 3. 3. LA TEORÍA DE LA SECURITIZACIÓN COMO MARCO TEÓRICO. 3.1. Título de la subsección tres punto uno. 4. OPERACIONALIZACIÓN Y METODOLOGÍA 5. ANÁLISIS 5.1 . La creación por Nixon de una Cuestión de Seguridad. 5.1.1. La creación de una Guerra Nacional contra las Drogas. 5.1.2. La virtualización de la frontera durante el mandato de Nixon. 5.2. Resultados y efectos aplicados de la securitización de Nixon 6. Conclusión. CONCLUSIÓN. 7. REFERENCIAS BIBLIOGRÁFICAS.

Resumen: Este trabajo investiga la evolución de la frontera entre Estados Unidos y México, que pasó de ser históricamente un límite simbólico para convertirse en una de las fronteras más fortificadas y tecnológicamente avanzadas del mundo. En las últimas décadas se ha observado una transformación significativa en las prácticas de control fronterizo, caracterizada por la integración de mecanismos de vigilancia digital que refuerzan las barreras físicas tradicionales. El estudio que se presenta aborda este fenómeno explorando el nexo entre la Guerra contra las Drogas de Nixon y la digitalización de la frontera entre Estados Unidos y México durante la Administración Nixon (1969–1974). Al conceptualizar la crisis de las drogas como una amenaza existencial, la retórica del presidente Nixon definió las definió como el "enemigo número uno", iniciando así su Guerra contra las Drogas. Comenzó así un proceso de securitización que permitió asignar recursos extraordinarios para contrarrestar esta nueva amenaza percibida. Mediante el uso de la teoría de la securitización desarrollada por la Escuela de Copenhague, se analiza el papel desempeñado por Nixon al enmarcar la amenaza de seguridad, con el fin de dilucidar cómo su discurso justificó la creación de prácticas de control fronterizo virtual en Estados Unidos. Los hallazgos sugieren que la securitización de la crisis de las drogas proporcionó la base necesaria para adoptar tecnologías innovadoras de vigilancia digital. Esta investigación contribuye al debate académico sobre la digitalización de fronteras y ofrece un marco metodológico para estudios comparativos sobre la evolución virtual de las fronteras nacionales.

Abstract: This paper investigates the evolution of the United States–Mexico border from a historically symbolic boundary into one of the most fortified and technologically advanced frontiers in the world. Initial symbolic physical demarcations placed along the border, served to formalise the division between the two nations. However, recent decades have witnessed a significant transformation in border enforcement practices, characterised by the integration of digital surveillance mechanisms that strengthen traditional physical barriers. This study addresses this phenomenon by exploring the nexus between Nixon's War on Drugs and the digitalisation of the US–Mexico border during the Nixon Administration (1969–1974). By conceptualising the drug crisis as an existential threat, President Nixon's rhetoric framed these substances as the "enemy number one" starting his War on Drugs. This shaped a securitisation process that enabled the allocation of extraordinary resources to counter this new perceived menace. By employing the securitisation theory developed by the Copenhagen School, this paper analyses the role played by Nixon in framing the security threat to elucidate how this discourse justified the creation of virtual border control practices in the United States.

The findings suggest that the securitisation of the drug crisis provided the necessary political and ideological foundation for adopting innovative digital surveillance technologies, a process that has since transformed border enforcement practices. This inquiry contributes to the academic debate on border digitalisation and offers a methodological framework for comparative studies on the virtual evolution of national boundaries.

Palabras clave: Frontera EE. UU.–México, Vigilancia Digital, Teoría de la Securitización, Guerra contra las Drogas, Administración Nixon

Keywords: US–Mexico Border, Digital Surveillance, Securitisation Theory, War on Drugs, Nixon Administration

1. INTRODUCCIÓN

La frontera que separa Estados Unidos (EEUU) de México es una de las más extensas del mundo. Un conjunto de montañas, desiertos y ríos caracterizan los 3.141 kilómetros de orografía que separan ambos países. Las primeras demarcaciones físicas de la frontera se introdujeron con el final de la Guerra México-Estados Unidos de 1847, que dio lugar al Tratado de Guadalupe (véase Trist *et al.,* 2022). Los cambios políticos introducidos por este Tratado se trasladaron al territorio mediante 52 montículos de piedra colocados de costa a costa a lo largo de todo el margen (US Customs and Border Protection, 2019). Mucho ha cambiado desde la separación simbólica que demarca el límite sur de los Estados Unidos (EE.UU.). Hoy se ha convertido en una de las fronteras más fortificadas y tecnológicamente avanzadas que existen.

El aspecto virtual de esta frontera es de especial interés para las prácticas de vigilancia que los países de todo el mundo llevan a cabo para asegurar sus bordes. De hecho, el potencial que tienen los sistemas de vigilancia contemporáneos en términos de control de los bordes nacionales ha sido objeto de numerosos estudios hasta fechas recientes (véase Adams, 2001; Amoore, Marmura, & Salter, 2008; Heyman, 2008). Sin embargo, poco se sabe sobre cuándo y por qué, en concreto, Estados Unidos decidió entrelazar los aspectos físicos y virtuales de sus fronteras para mejorar el control sobre ellas. Se trata de un paréntesis desconcertante, especialmente si se tiene en cuenta la posición de liderazgo de Estados Unidos en cuanto al arsenal digitalizado empleado a lo largo de la frontera entre Estados Unidos y México, junto con una consideración más bien escasa de dónde empezó todo.

Las investigaciones demuestran que existe un vínculo entre la guerra de Vietnam y la implantación por parte de EE.UU. de mecanismos de aplicación de la ley virtuales a lo largo de la frontera entre EE.UU. y México (véase Barkan, 1972; Grandin, 2019; Rosenau, 2001). Sin embargo, no se ha prestado suficiente atención al nexo que une estos dos acontecimientos separados de la historia estadounidense. Para ser más precisos, el nexo en cuestión es la Guerra contra las Drogas de Nixon. Fue al describir las drogas como el enemigo número uno de los Estados y declarar una guerra total contra las drogas en 1971 cuando el Presidente consiguió abrir una ventana para la digitalización de la frontera sur. Al abordar la siguiente pregunta de investigación, este artículo pretende llenar este vacío en la literatura académica: ¿Cómo contribuyó la Guerra contra las Drogas bajo la Administración Nixon a la transición de un control fronterizo físico a lo largo de la frontera sur a mecanismos de aplicación virtuales?

Una herramienta valiosa para encontrar una respuesta a esta pregunta la ofrece la teoría de la titulización. Esta teoría fue impulsada por la Escuela de Copenhague y ofrece un marco teórico que puede utilizarse para identificar patrones en el proceso de securitización de un asunto que otorga recursos extraordinarios para contrarrestarlo. En esta investigación, estos patrones dilucidados por uno de los principales componentes de la Escuela, Wæver (1995), se aplican a los comentarios de Nixon sobre la Guerra contra las Drogas y la posterior inversión en activos digitales para la frontera sur de Estados Unidos.

Este estudio sostiene que el discurso que Nixon enmarcó sobre las drogas como una amenaza nacional permitió a Estados Unidos avanzar en la virtualización de la frontera México-Estados Unidos. El marco temporal objeto de análisis de este trabajo coincide

con el mandato de la Administración Nixon, es decir, de 1969 a 1974. Establecer en qué momento exacto y de qué manera Estados Unidos logró iniciar su fortificación fronteriza virtual es valioso para el debate académico. Esto es así porque los resultados de esta investigación pueden utilizarse para comparar el desarrollo tecnológico en los estudios fronterizos de otros países también durante sus fases iniciales de virtualización de fronteras.

Para desarrollar la investigación con diligencia, este documento se divide en las siguientes secciones. La primera sección da cabida a la revisión bibliográfica sobre los enfoques teóricos más relevantes que se han adoptado para realizar estudios sobre las fronteras virtuales. La segunda sección presenta la teoría de la securitización como el marco teórico adoptado por este estudio para llevar a cabo su análisis. La tercera sección resume la operacionalización y la metodología utilizadas para formalizar esta investigación. La cuarta sección se compone del análisis de este estudio. En esta sección, los principios de la teoría de la titulización se aplican a dos discursos emblemáticos de Nixon. A continuación, se comentan las conclusiones resultantes basándose en el respaldo de fuentes secundarias. La última sección propone una conclusión que resume los hallazgos y consideraciones alcanzados a lo largo del presente estudio.

2. REVISIÓN BIBLIOGRÁFICA SOBRE FRONTERAS Y VIGILANCIA VIRTUAL

Hay una serie de teorías que se utilizan para apreciar los diversos fundamentos de las fronteras y sus pautas de transformación. En lo que respecta específicamente a los procesos de virtualización de las fronteras, el alcance de las teorías que se aplican se reduce considerablemente. Para identificar lo que se ha escrito sobre la relación de las fronteras y su digitalización en función de las necesidades políticas, cuatro teorías principales consiguen captar la atención. Esta sección está dedicada a discutir estas distintas contribuciones académicas. Cada una de ellas aporta una visión diferente al tema de investigación del estudio y puede servir para comprender su origen.

Michel Foucault impulsó una perspectiva más filosófica de los estudios sobre la vigilancia. Al revisar la teoría del filósofo francés, Lemke (2015) afirmó que "la obra de Foucault sobre la gubernamentalidad no sólo ofrece importantes perspectivas para un análisis del Estado, sino que también proporciona herramientas analíticas para investigar la relación entre lo liberal y las tecnologías de seguridad" (p. 5). Más concretamente, la teoría foucaultiana de la gubernamentalidad describe cómo los Estados emplean el poder a través de técnicas disciplinarias y de vigilancia en lugar de la fuerza directa (Lemke, 2015). Esta teoría analiza la dimensión extraterritorial del control fronterizo gestionado por actores estatales que puede ir más allá de la demarcación física de su propio país.

Esta idea resulta atractiva para entender la digitalización de las fronteras, ya que puede aplicarse a las prácticas estatales que contrarrestan las amenazas a la seguridad nacional reinterpretando las demarcaciones físicas. La idea que subyace a esta teoría es intentar bloquear riesgos específicos antes de que lleguen a la frontera. Para ser más precisos, las leyes nacionales pueden utilizarse para impulsar cambios gubernamentales que contemplen la informatización de las cuestiones de seguridad que amenazan la seguridad nacional. De este modo, los Estados pueden avanzar hacia un sistema de vigilancia cada vez más virtual, utilizado para controlar y eliminar los peligros antes de que consigan entrar en su territorio (véase Armstrong, 1992; Paden, 1984). Esta corriente

de acciones pone de relieve cómo pueden cambiar las fronteras convencionales una vez que las configuraciones virtuales se integran en las prácticas de control fronterizo.

La teoría foucaultiana de la gubernamentalidad, sin embargo, se queda corta cuando se aplica a la investigación de la securitización fronteriza relacionada con las drogas. Aunque la teoría menciona el protagonismo tecnológico en la creación de fronteras, se dirige principalmente a un estudio de la vigilancia y el control en lugar de centrarse en la securitización fronteriza *per se*. Esta teoría es incapaz de explicar por qué los responsables políticos actúan cuando se enfrentan a acontecimientos imprevistos, como fue el caso de la crisis de la droga de los años sesenta en Estados Unidos. En esta línea, Kerr (1999) llegó a la conclusión de que la teoría no puede "dar cuenta de los límites cambiantes del gobierno, aparte de señalar el mero hecho de que el gobierno a menudo fracasa debido a resultados no planificados " (p. 196). Así pues, aunque esta gubernamentalidad foucaultiana ha demostrado ser pionera en la virtualización de las fronteras, no permite dar una respuesta exhaustiva a la pregunta de investigación que orienta el presente estudio.

Otra teoría relevante utilizada para analizar las fronteras inteligentes es el determinismo tecnológico. Esta teoría basa sus fundamentos en la identificación de los avances tecnológicos como impulsos sociales y políticos. En particular, subraya la importancia que tiene la tecnología en la configuración de los cambios políticos. En palabras de Smith (1994) "el poder de la tecnología [es] un agente crucial de cambio [que] ocupa un lugar destacado en la cultura de la modernidad" (p. ix). Según esta teoría, el empuje que hace que se produzcan las novedades no es impulsado por las personas, sino por la propia tecnología. Ésta, a su vez, provoca cambios que primero se presentan en la agenda política y luego son aplicados por los responsables políticos.

De este modo, las transformaciones fronterizas se entienden como el resultado de avances tecnológicos y no de impulsos sociopolíticos. En este sentido, el auge de la vigilancia electrónica junto con el rastreo biométrico y la teledetección hicieron viable en primer lugar la aplicación virtual de la ley. Por lo tanto, vinculando esta perspectiva a la pregunta de investigación de este artículo, las estrategias de represión antidroga evolucionaron como resultado de las posibilidades tecnológicas en lugar de las decisiones políticas. En consecuencia, los políticos estadounidenses se vieron empujados, en lugar de impulsar el cambio tecnológico, a aplicar la represión fronteriza virtual para contrarrestar la entrada de drogas en el país.

Aunque el determinismo tecnológico consigue aportar ideas relevantes sobre el cambio de los regímenes fronterizos, se le ha señalado por simplificar en exceso este proceso. Se discute en gran medida que los miembros sociales y políticos también son capaces de influir en la tecnología en lugar de estar a su merced. Es decir, una comprensión más profunda de la tecnología ha permitido controlarla (Dafoe, 2015, p. 1049; Lynch, 2008). En consecuencia, el aspecto digital de las fronteras no es el resultado del impulso tecnológico, sino que está controlado por los políticos. De ahí que pueda considerarse que la adaptación de la frontera sur de EE.UU. durante el mandato de Nixon adoptó un claro giro tecnológico. Sin embargo, este giro fue controlado por acciones dirigidas por hombres, lo que hace difícil confiar en el determinismo tecnológico para la investigación que propone este documento.

La composición digital de las fronteras también puede entenderse mediante la teoría fronteriza de Nail. Esta teoría ofrece una visión de la frontera que ve una cualidad móvil y dispersa cada vez mayor en las fronteras físicas convencionales. En opinión de Nail (2016), "la frontera no es reducible a la definición clásica de los límites de un Estado soberano" (p. 2). Las fronteras, observó el autor, evolucionan inevitablemente hacia una identidad informacional o digital que afecta a la comprensión social de un país. Esto significa que las fronteras han adoptado una forma virtual, ya que los problemas modernos afectan a la circulación transfronteriza de personas y bienes, a los que se exige respuestas actualizadas. En el caso del tráfico de drogas en Estados Unidos, por ejemplo, los nuevos métodos adoptados por los cárteles exigieron acciones innovadoras por parte del control fronterizo estadounidense para contrarrestar esta tendencia. En los años sesenta y setenta, estas acciones se redujeron a la transformación de las fronteras en espacios de control en red.

La teoría de las fronteras, por tanto, elude la concepción convencional de las fronteras como tales. En lugar de centrarse exclusivamente en su aspecto territorial y físico, como dilucidó Sharma (2023, pp. 163-164), es necesario ampliar esta concepción a los bienes intangibles que componen las fronteras de los Estados. Las implicaciones que plantea esta teoría añaden una nueva dimensión al poder de los gobiernos. Es decir, las fronteras no deben verse como una simple línea , sino como una amplia zona que rodea la demarcación física (Nails, 2016). De hecho, los Estados pueden llegar mucho más allá de sus límites físicos mediante mecanismos de aplicación virtuales con el objetivo de securitizar sus fronteras. Modelos prácticos de ello son las bases de datos de la Patrulla Fronteriza estadounidense y las redes de intercambio de inteligencia que se han utilizado en gran medida para proteger su frontera sur. En la década de 1970, estos sistemas de la Patrulla Fronteriza lideraron ampliaciones que allanaron el camino para las actuales estructuras digitales de aplicación de la ley en las fronteras.

La teoría de las fronteras defiende la idea de que los Estados pueden vigilar los movimientos más allá de sus propias fronteras. Las delimitaciones territoriales, según esta concepción, pierden relevancia para los gobiernos a la hora de tomar medidas relacionadas con la vigilancia de fronteras (Sharma, 2023. P. 164). Aunque siguen representando un aspecto importante de la formulación de políticas fronterizas, los gobiernos tienden a actuar más allá de la delimitación territorial con la idea de interceptar posibles amenazas. Dicho de otro modo, la prevención adquiere tanta relevancia como la disuasión física. Los escollos de esta mentalidad son las intervenciones políticas extraterritoriales que tienen muchas posibilidades de dañar las relaciones internacionales. Esta teoría resulta útil para comprender el cambio general de la conceptualización de la frontera sur de Estados Unidos. Sin embargo, puede utilizarse para estudiar la separación social, aunque carece de un vínculo claro con las cuestiones de seguridad fronteriza.

Para entender las fronteras desde un punto de vista relacionado con la seguridad, hay que tener en cuenta la teoría de la securitización de la escuela de Copenhague. Otukoya (2024, p. 1750) observó que la creación de un problema de seguridad puede ser clave para crear recursos extraordinarios utilizados para proteger a una nación de un peligro imaginario. Esta teoría es útil para comprender cómo se utilizan las características digitales para reforzar el aspecto físico de la frontera. Aquí la atención se centra, entre otras cosas, en los sensores de movimiento, la videovigilancia y cualquier otra característica tecnológica que se utilice para vigilar la frontera territorial con mayor

efecto. Por lo tanto, se presenta como el marco teórico adecuado necesario para identificar tales patrones a lo largo de la frontera sur de Estados Unidos.

Al analizar los inicios de la Guerra contra las Drogas, maniobras como la Operación Intercepción, emprendida en 1969, se justificaron como una acción necesaria para luchar contra el enemigo público número uno de Estados Unidos en aquella época. En esta operación, se empezaron a necesitar nuevas formas de vigilancia electrónica de las fronteras por primera vez en la historia del régimen fronterizo estadounidense. Estas necesidades personifican los pilares fundacionales de la compleja dimensión tecnológica que caracteriza la frontera contemporánea del país. Dada la estrecha relación que guarda esta teoría de la securitización con los objetivos de esta investigación, es preciso profundizar en su composición. En la siguiente sección, se resume la teoría de la titulización. Esto permite encontrar indicadores clave para comprender cómo cambió la securitización de la frontera estadounidense durante la Administración Nixon adoptando un aspecto virtual.

3. LA TEORÍA DE LA TITULIZACIÓN COMO MARCO TEÓRICO

La teoría de la securitización es un marco útil que puede utilizarse para comprender la seguridad fronteriza en Estados Unidos durante la presidencia de Nixon. La función general de esta teoría es explicar cómo las cuestiones llegan a dirigir el proceso de toma de decisiones de un país en asuntos como el control de fronteras. Aplicada al estudio que nos ocupa, esta teoría parece ser de gran ayuda para comprender los mecanismos de control virtuales que EE.UU. ha añadido a su frontera física meridional. Aplicando la teoría de la securitización a este tema, el presente estudio pretende dilucidar el papel que desempeñó el Presidente Nixon al contribuir a la implantación de una frontera virtual. Esta sección está dedicada a señalar los principales principios de la teoría de la securitización para poder aplicarlos formalmente al análisis del documento.

La escuela de Copenhague basó su teoría en cinco pilares principales. Los pilares en cuestión son (1) la securitización como acto de habla, (2) el encuadre elitista de las amenazas, (3) el requisito de aceptación de la audiencia, (4) la identificación del objeto referente, y (5) la reversibilidad y la desecuritización. Todos estos factores combinados pueden utilizarse en el análisis de este documento para descubrir cómo la Guerra contra las Drogas de Estados Unidos contribuyó a la transición del control físico de las fronteras a los mecanismos virtuales de aplicación de la ley. No obstante, antes de entrar en el análisis, se resume y contextualiza cada indicador para aclarar de qué manera se utiliza después aplicado al estudio de caso de la revisión.

Declarar un asunto como amenaza para la seguridad constituye un acto performativo emprendido por un gobierno. Con esta concepción de la seguridad, Ole Wæver -el cerebro de la teoría de la titulización- descubre un acto performativo que los gobiernos asumen cuando indican al público la presencia de un problema relacionado con la seguridad (Wæver, 1995, p. 52). Al dirigir la atención hacia un problema, una élite puede llevar a cabo una actuación que abre una ventana para la adopción de medidas políticas excepcionales destinadas a detener un determinado contratiempo. Es irrelevante si este asunto representa un problema ordinario o una amenaza real para la seguridad nacional. Lo que importa es que el público concede a los representantes del Estado una considerable libertad de acción que legitima sus actuaciones. Es lo que se denomina acto de habla.

Los actos de habla se basan en la creación vertical de confianza entre los funcionarios del Estado y los ciudadanos. El éxito de un acto de habla depende de la medida en que una promesa o una declaración sea aceptada por el público. Los representantes del Estado se aprovechan del sentimiento de confianza que los ciudadanos les otorgan para crear una nueva realidad política cuya existencia depende de la cuestión de la seguridad concebida. Es mediante el empleo de actos de habla como se revela la legitimación para tomar medidas que hagan frente a las amenazas a la seguridad. Esta legitimación, a su vez, permite movilizar el desbloqueo de los recursos estatales creando acciones que van más allá de los procedimientos normales y permiten la formación de medidas extraordinarias (Wæver, 1995, p. 53).

Sin embargo, esta práctica no está exenta de riesgos. Wæver (1995) subraya que es así porque dificulta la distinción entre el acto y el grado real de amenaza al que se enfrenta un país (p. 6). En otras palabras, el Estado puede convertirse en víctima de su propia narrativa al dar demasiada importancia a un asunto que en realidad no supone un peligro real para la seguridad de la nación. Al hacerlo, puede producirse el efecto contrario de comprometer la seguridad del país al centrarse demasiado en un problema inexistente y descuidar sus verdaderas prioridades.

El segundo indicador recuperado en la teoría de la titulización es la práctica de las élites de enmarcar las amenazas. La teoría de la securitización subraya la influencia que tienen los actores clave en la configuración de las acciones políticas. Este proceso lo inician estos pocos elegidos que tienen una influencia significativa dentro de los rangos políticos superiores. Una vez que estos individuos consiguen crear una narrativa de la amenaza, asumen el poder de definir lo que puede definirse como peligros existenciales para la seguridad del país. El resultado es una acción estatal cohesiva destinada a atajar el problema derivado de la creación de esa misma narrativa.

No obstante, la autoridad que ostenta la élite es un arma de doble filo. Por un lado, permite crear una reacción estatal rápida (Wæver, 1995, p. 54). Esto es especialmente positivo, ya que a menudo los Estados están limitados por una burocracia enrevesada que prolonga considerablemente el tiempo de aplicación de las medidas oficiales. Por otro lado, este dominio permite a las élites eludir los procesos democráticos convencionales (Wæver, 1995, p. 54). Esto significa que, al acelerar el normalmente lento proceso de elaboración de políticas, sólo unos pocos seleccionados concentran en sus manos el poder de decisión. La implicación de esta concentración de poder permite a la élite no sólo decidir cómo hacer frente a las amenazas a la seguridad, sino también decidir qué debe considerarse una amenaza y qué no. Así, el encuadre de las cuestiones de seguridad puede vincularse fácilmente a los intereses estratégicos que tienen las élites (Wæver, 1995, p. 54). En otras palabras, las élites pueden decidir si actúan para garantizar la seguridad pública o los intereses personales.

Esto nos lleva al tercer indicador: el requisito de aceptación por parte del público. Los movimientos de securitización, según la escuela de Copenhague, dependen de la aceptación por parte de las audiencias relevantes. Los principales públicos de interés para la élite son la opinión pública, los órganos legislativos o los socios internacionales. Todos ellos -independientemente o no- deben confiar en la veracidad de la narrativa construida sobre la amenaza para crear el *impulso* necesario para emprender acciones prácticas. Éstas, a su vez, sostenía Wæver (1995, p. 53), permiten encontrar una solución a la amenaza propuesta. Sin la aceptación de la audiencia, incluso las reivindicaciones de

seguridad enunciadas de forma más convincente pueden tambalearse. De ahí que la no aceptación de una cuestión de seguridad resulte contraproducente y genere un proceso de desecuritización. El esfuerzo de la élite se desvanecería así a costa de sus intereses estratégicos (Wæver, 1995, pp. 53-54). Por ello, el indicador de exigencia de aceptación de la audiencia se propone como un factor esencial. Es necesario analizar en qué medida la aprobación o el desafío del público a procedimientos inusuales puede autorizar o hacer mella en el alejamiento de las prácticas tradicionales y democráticas.

El cuarto indicador que compone la teoría de la titulización puede identificarse con la identificación del objeto de referencia. El proceso de titulización necesita una especificación clara de lo que está en juego. Lo que está en juego, en este caso, se denomina objeto de referencia. Según Wæver (1995, p. 52), el objeto de referencia suele identificarse con la integridad del Estado, la soberanía o la seguridad de sus ciudadanos. El proceso de definición del objeto de referencia es fundamental para la movilización de recursos. De hecho, una clara delimitación del objeto trazada por los actores securitizadores desbloquea los medios materiales necesarios para defender esa entidad concreta frente a supuestas coacciones existenciales (Wæver, 1995, pp. 52-53). Esta definición clara es fundamental para condonar el uso de acciones excepcionales, ya que determina lo que debe defenderse por todos los medios.

La reversibilidad y la desecuritización encarnan el último indicador de la teoría de la titulización. Según la escuela de Copenhague, la securitización está sujeta a cambios constantes. Una vez que el público comprueba que una amenaza a la seguridad ha dejado de ser existencial, puede revertir las medidas de securitización adoptadas hasta el momento y volver a transformar la cuestión en un debate político normal (Wæver, 1995, p. 55). Esta retracción permite poner en jaque a la élite que enmarcó la cuestión. Esta reversibilidad pone de relieve cómo las respuestas de emergencia temporales pueden ser desmontadas después de haber experimentado una acumulación momentánea. De ahí que Wæver (1995, pp. 54-55) sugiriera que el acto de titulización conlleva riesgos intrínsecos que son inherentes al proceso de titulización. Dicho de otro modo, las medidas de titulización pueden surgir y desvanecerse con facilidad, lo que dificulta la predicción de las futuras medidas que puede adoptar un gobierno en el ámbito de la seguridad.

En general, los principios que conforman la teoría de la titulización propuesta por la escuela de Copenhague son herramientas analíticas valiosas. Éste es concretamente el caso del tema de investigación de este documento. La aplicación de las herramientas analíticas puestas a disposición por esta teoría puede facilitar la comprensión de cómo la Guerra contra las Drogas puede haberse transformado en una cuestión de seguridad utilizada para crear espacio para medidas excepcionales. De hecho, , los principios enumerados en esta sección ayudan a evaluar la transformación de las prácticas delictivas convencionales -como el contrabando y el consumo de drogas- y los problemas de salud en medidas excepcionales adoptadas por los Estados para hacer frente a estas cuestiones. Se produjeron cambios significativos en las políticas gracias a los discursos de las élites que dieron lugar a políticas inéditas que desembocaron en la adopción de mecanismos virtuales de aplicación de la ley para luchar contra el narcotráfico a lo largo de la frontera sur de Estados Unidos. La siguiente sección expone la operacionalización y la metodología que este documento adopta para llevar a cabo su análisis.

4. OPERACIONALIZACIÓN Y METODOLOGÍA

Toshkov (2016, p. 100) describió la operacionalización como la traducción de conceptos abstractos en nociones concretas que pueden observarse, clasificarse y medirse empíricamente. Los principios que componen la teoría de la titulización pueden utilizarse con el mismo propósito. En este trabajo se han operacionalizado cuatro de los cinco conceptos clave para comprender el papel que tuvo la Guerra contra las Drogas a la hora de contribuir a la transición de Estados Unidos hacia las fronteras virtuales. Los cuatro indicadores que componen la teoría y que se utilizan en este documento para analizar el caso de estudio son: (1) la securitización como acto de habla, (2) el encuadre elitista de las amenazas, (3) el requisito de aceptación de la audiencia y (4) la identificación del objeto referente. El último principio señalado en la teoría de la securitización -la reversibilidad y la desecuritización- no es útil para esta investigación. Es decir, este último principio es útil para estudiar la deconstrucción de una medida de seguridad, una parte que este estudio no pretende abarcar. No obstante, esto no compromete la solidez de este trabajo, ya que las pautas que conducen a la titulización permanecen inalteradas.

Los cuatro indicadores permiten profundizar en la dimensión virtual que adquirió la frontera sur de EEUU durante el mandato de Nixon. En consecuencia, se impulsa una reflexión cualitativa crítica sobre el tema de investigación para comprender la importancia que tiene en la actualidad para EEUU potenciar la digitalización a lo largo de su frontera territorial que le separa de México. Los cinco indicadores, por lo tanto, son de fundamental importancia para identificar por qué la crisis de la droga logró personificar un factor clave en los mecanismos de aplicación de la frontera virtual.

También hay que aclarar la metodología de este trabajo. Esta investigación consiste en un único estudio de caso. Más concretamente, analiza la frontera sur de Estados Unidos durante la presidencia de Nixon. Los estudios de caso único permiten dar información precisa sobre un caso concreto para crear conocimientos que luego puedan aplicarse también a casos similares. Es decir, con esta investigación, el modelo de investigación puede utilizarse luego en casos similares para identificar patrones análogos de evolución en el control virtual de fronteras. La decisión de optar por este estudio de caso se basa en el hecho de que EE.UU. se encuentra entre los primeros países que decidieron optar por la digitalización parcial de su frontera. Por lo tanto, la justificación de la selección del caso reside en el interés por añadir nueva información al vacío de investigación académica que existe sobre este tema.

A lo largo del análisis del tema se utilizan diversas fuentes primarias y secundarias. El objetivo de disponer de un amplio abanico de información procedente de diversas fuentes contribuye a consolidar y garantizar la calidad de las conclusiones de esta investigación. Al igual que en las fuentes primarias, se tienen en cuenta las declaraciones políticas, los artículos periodísticos y los discursos públicos. En estas fuentes pueden reconocerse rasgos importantes relativos a la teoría de la titulización. Mientras que las fuentes secundarias utilizadas en este estudio proceden de estudios académicos que se han llevado a cabo sobre el tema de la seguridad fronteriza, la seguridad virtual y la Guerra contra las Drogas. Se trata de una práctica útil que permite situar las conclusiones del estudio en un debate académico más amplio.

El análisis del discurso representa la columna vertebral de este estudio. Se examina la información extraída de dos discursos pronunciados por Nixon en relación con la

Guerra contra las Drogas. Basándose en un método cualitativo, la interpretación de las fuentes dadas ayuda a identificar los indicadores presentados en el marco teórico. Los discursos políticos pronunciados por el presidente estadounidense son, por tanto, clave para completar este estudio. Además, aplicando este método de investigación, es posible poner a prueba la teoría empleada en este estudio. En efecto, al aplicar los indicadores propuestos por la teoría de la titulización a los discursos, es posible comprender si realmente existen patrones en los discursos políticos que puedan conducir a la titulización de los riesgos construidos.

El marco temporal de esta investigación se basa en el mandato de la Administración Nixon. Más concretamente, el tiempo considerado abarca desde 1969 hasta 1974. Este reducido marco temporal ayuda a dar espacio a una serie de acciones clave emprendidas por el Presidente de EE.UU. de la época en relación con los mecanismos de control virtual a lo largo de la frontera entre EE.UU. y México.

5. ANÁLISIS

5.1. LA CREACIÓN DE UN PROBLEMA DE SEGURIDAD POR PARTE DE NIXON

La vigilancia de la frontera que separa México de Estados Unidos entre 1969 y 1974 se centró predominantemente en el tráfico ilegal de drogas. La región de Sinaloa, en el noroeste de México, arrancó el cultivo de opio a los inmigrantes chinos en la década de 1910. Desde entonces, el cártel de Sinaloa se enriqueció exportando esta sustancia principalmente a Estados Unidos. Sin embargo, con la generación hippie y el tráfico de marihuana, la importación ilegal de sustancias a EE.UU. se convirtió en un problema para la sociedad (Grillo, 2013, p. 255). El problema de las drogas se convirtió en el tema central en torno al cual el presidente Nixon basó la mayor parte de su actividad política. Más allá de esto, Timmons (2017, p. 15) llamó la atención sobre el hecho de que Richard Nixon se convirtió en el primer presidente que hizo la promesa de cerrar la frontera entre Estados Unidos y México a las drogas ilegales. De hecho, mientras la guerra en Vietnam continuaba, "la Administración Nixon está americanizando silenciosamente la tecnología de la guerra, y la guerra en el frente interno se intensifica" (Barkan 1972, p. 1).

Para profundizar en el papel que desempeñó Nixon en el inicio de esta tendencia, la primera parte del análisis se dedica al análisis del discurso de dos discursos del Presidente en cuestión. Las comunicaciones en cuestión son *Remarks About an Intensified Program for Drug Abuse Prevention and Control (Observaciones sobre un programa intensificado de prevención y control del abuso de drogas*) y *Special Message to the Congress on Drug Abuse Prevention and Control (Mensaje especial al Congreso sobre prevención y control del abuso de drogas*). Ambos discursos tuvieron lugar el 17 de junio de 1971. Ambos discursos tuvieron lugar el mismo día y se sucedieron. De hecho, el primero personifica la conferencia de prensa celebrada para explicar lo que mencionó durante su discurso al Congreso.

Ambos discursos son clave para entender de qué manera se propuso a la audiencia política y pública el encuadre elitista de una amenaza. Mirándolos con detenimiento es posible comprender cómo Nixon consiguió desbloquear recursos extraordinarios para contrarrestar la nueva y construida amenaza existencial de las drogas en EEUU. Ambos discursos se presentan conjuntamente en un documento facilitado por el Departamento de Defensa de EEUU (2017). Tras identificar los puntos más relevantes de ambos, se procede

a esclarecer la relevancia que estas singulares medidas han tenido en el proceso de virtualización de la frontera sur de EEUU entre 1969 y 1974.

5.1.1. La creación de una Guerra Nacional contra las Drogas

Al considerar los discursos de Nixon desde el punto de vista de la teoría de la securitización, es necesario buscar un acto performativo. Este acto debe llamar la atención de la audiencia sobre la existencia de un problema relacionado con la seguridad que pone en peligro su bienestar. El Presidente Nixon lo hizo declarando audazmente una guerra total contra las drogas. En la rueda de prensa que ofreció, tras dirigirse al Congreso con un mensaje especial, abrió su comunicación afirmando que "el enemigo público número uno en Estados Unidos es el abuso de drogas" (Departamento de Defensa de Estados Unidos, 2017, p. 1). Una apertura tan rimbombante resultó cautivadora para el público espectador. Ayudó a crear una sensación de miedo entre la población estadounidense que llevaba 15 años en la catastrófica guerra de Vietnam. No es de extrañar que cualquier referencia a amenazas a la seguridad nacional, guerras y enemigos en aquellos años despertara fácilmente sentimientos de paranoia y el deseo de actuar.

Para proponer la nueva amenaza, Nixon tuvo que señalar en qué consistía realmente. Lo hizo afirmando que:

> Existen varias grandes categorías de drogas: las de la familia del cannabis, como la marihuana y el hachís; las que se utilizan como sedantes, como los barbitúricos y ciertos tranquilizantes; las que elevan el estado de ánimo y suprimen el apetito, como las anfetaminas; y drogas como el LSD y la mescalina, que suelen denominarse alucinógenos. Por último, están los analgésicos narcóticos, como el opio y sus derivados, la morfina y la codeína. La heroína se fabrica a partir de la morfina". (Departamento de Defensa de EE.UU., 2017, p. 10).

Esto es lo que la teoría de la securitización identifica con la identificación del objeto referente. Al señalar e insistir en quién o qué representa una amenaza, el público puede identificar el problema e impulsar acciones contra él.

Además, representarse a sí mismo como un Presidente prudente ayudó a que el acto performativo resultara más convincente. De ahí que declarara que "Dudo mucho siempre en traer alguna nueva responsabilidad a la Casa Blanca, [...] pero considero que este es un problema tan urgente [...] que había que traerlo" (Departamento de Defensa de EE. UU., 2017, p. 2). Con ello, Nixon intentaba presentarse como el protector y garante de los EE.UU. cuyas acciones estaban guiadas por las necesidades de los ciudadanos estadounidenses y no por intereses personales.

Se crearon una serie de medidas excepcionales para hacer frente a esta amenaza a la seguridad nacional. Nixon afirmó que "es necesario librar una nueva ofensiva total" (Departamento de Defensa de EE.UU., 2017, p. 1), evocando la necesidad de un esfuerzo común para detener un peligro que había logrado penetrar en suelo estadounidense. Estas palabras aclaraban hasta qué punto Estados Unidos estaba comprometido a luchar activamente contra las amenazas a la seguridad relacionadas con las drogas. La aplicación de medidas de tipo bélico, como el despliegue y la creación de departamentos militares y federales para controlar y combatir las rutas de la droga que se dirigen a Estados Unidos, personificaba la base de este nuevo plan de acción.

En este punto, es necesario destacar la aceptación del público del acto discursivo de Nixon. De hecho, es posible afirmar que el público aceptó su discurso adoptado con la Guerra contra las Drogas. Señal de esta aceptación son una serie de acciones propuestas por la Administración y luego ejecutadas con el apoyo general de la mayoría del país. La operación más emblemática que dio inicio a la Guerra contra las Drogas fue la Operación Intercepción lanzada a lo largo de septiembre y octubre de 1969. Esta operación tuvo como resultado el cierre casi completo de la frontera entre México y EEUU.

La Operación Intercepción presentó una debacle debido a la imposibilidad de controlar toda la frontera mediante disposición física. Aunque se desplegaron dos mil agentes de aduanas, no se consiguieron resultados efectivos (véase Reid, 2022). No obstante, el apoyo público y político cedió para nuevas acciones que abrieron la puerta a nuevos tipos de procedimientos. Este fue el caso de la Comprehensive Drug Abuse Prevention and Control Act (CDAPC Act) de 1970, adoptada para reforzar el control estadounidense, entre otras cosas, a lo largo de la frontera sur.

La Operación Interceptación y la Ley CDAPC representan los hitos en los que se basaron sus discursos de 1971. De hecho, estas acciones desencadenaron una serie de procedimientos gubernamentales adicionales para intensificar la Guerra contra las Drogas. Un indicador de cómo el presidente Nixon quería aumentar estos procedimientos destinados a detener esta amenaza a la seguridad es visible en el siguiente pasaje: "Ahora debemos reconocer con franqueza que los procedimientos deliberados encarnados en los esfuerzos actuales para controlar el abuso de drogas no son suficientes en sí mismos. El problema ha adquirido las dimensiones de una emergencia nacional" (Departamento de Defensa de Estados Unidos, 2017, p. 3). Fue así como logró obtener el apoyo bipartidista para hacer frente a esta nueva y aparentemente devastadora amenaza a la seguridad.

Para ser más precisos, las medidas legislativas más importantes adoptadas desde los dos discursos analizados en esta sección fueron: la fundación por Orden Ejecutiva de la Oficina de Acción Especial para la Prevención del Abuso de Drogas en 1971, la ampliación de la Ley de Rehabilitación de Toxicómanos de 1966 en 1971, la organización de la Ley de Asistencia para la Seguridad Internacional de 1971 junto con la Ley de Desarrollo Internacional y Asistencia Humanitaria de 1971, la creación de la Oficina de Aplicación de la Ley contra el Abuso de Drogas en 1972 y la creación de la Administración para el Control de Drogas (DEA) en 1973.

Es importante subrayar que este tipo de acciones sólo eran posibles con un amplio apoyo político. El Presidente era consciente de este rasgo, ya que a lo largo de su conferencia de prensa se centró repetidamente en el apoyo bipartidista de sus acciones. Se trata de un aspecto importante a la hora de considerar la teoría de la securitización, ya que subraya el poder que la aceptación general otorga a la élite que enmarca la amenaza a la seguridad. Un poder que permite a la élite emprender acciones extraordinarias en poco tiempo, algo que choca con los largos procedimientos burocráticos que en estas situaciones quedan anulados.

Más allá del apoyo político, Nixon consiguió que la sociedad aceptara la amenaza que logró enmarcar. Lo hizo subrayando cómo cualquier miembro de la sociedad estadounidense se veía afectado por la amenaza de las drogas. Al afirmar que "En 1960, se registraron menos de 200 muertes por narcóticos en la ciudad de Nueva York. En 1970, la cifra había aumentado a más de 1.000" (Departamento de Defensa de EE.UU., 2017,

p. 2) Nixon logró establecer una relación vertical entre el autor del acto de discurso y su audiencia. El punto que el Presidente de los EE.UU. hizo aquí es que la población media de los EE.UU. estaba cayendo a las drogas. Se trata de un punto convincente con el que la gente pudo identificarse, ya que estaba ocurriendo cerca de ellos. El esfuerzo por convencer a su audiencia ejemplifica otro aspecto fundamental mencionado en la teoría de la securitización. Es decir, desvela cómo los miembros de la élite intentan crear un tema y lograr su reconocimiento entre un público amplio.

Una situación similar se describe en el mismo discurso en el que Nixon intentó pedir una respuesta comunitaria aprovechando los sentimientos individuales. La frase en cuestión es: "Para derrotar a este enemigo, que está causando tanta preocupación, y con razón, a tantas familias estadounidenses, se proporcionará dinero" (Departamento de Defensa de EE. UU., 2017, p. 1). Lo que el presidente estadounidense intentó hacer aquí fue asegurarse el favor definitivo de su audiencia. Es mediante declaraciones como esta como se logra la legitimación y, por tanto, debe considerarse como una parte inherente del proceso de enmarcado de la amenaza en la securitización.

El proceso de legitimación era necesario para emprender acciones en las fronteras de EEUU e incluso más allá. Como él mismo dijo: "Ningún ataque serio a nuestro problema nacional de drogas puede ignorar las implicaciones internacionales de tal esfuerzo, ni el esfuerzo nacional puede tener éxito sin atacar el problema en un plano internacional" y luego "estoy iniciando una escalada mundial en nuestros programas existentes para el control del tráfico de narcóticos" (Departamento de Defensa de EE.UU., 2017, p. 11). Estas acciones estaban dirigidas principalmente a quienes introducían drogas en suelo estadounidense. En palabras del presidente: "detener el tráfico de drogas golpeando a los productores ilegales de drogas [...] y el tráfico de estas drogas más allá de nuestras fronteras" (p. 4). En otras palabras, Nixon enmarcó a los narcotraficantes extranjeros como una amenaza ampliando el alcance de quién era la raíz de la causa que producía la amenaza que ponía en peligro la seguridad de EEUU. Estos fueron aspectos clave que, a partir de entonces, darían forma a las relaciones exteriores del país, especialmente con los estados situados por debajo de su frontera sur.

Los discursos utilizados para este análisis del discurso resultaron útiles para identificar los patrones propuestos por la teoría de la securitización. Al dirigirse al Congreso y a la población estadounidense con discursos posteriores, el presidente Nixon consiguió revigorizar la transformación del problema de las drogas en una cuestión de seguridad persistente. De este modo, los indicadores de la teoría de la securitización ayudaron a trazar la evolución de un problema criminal y de salud pública relativamente convencional a otro que reivindicaba cambios sustanciales en las políticas. Con el objetivo de ampliar el proceso de securitización emprendido por EE.UU. para introducir mecanismos virtuales de aplicación de la ley en su frontera territorial sur entre 1969 y 1974, la siguiente sección examina una serie de fuentes secundarias que se han escrito sobre este tema.

5.1.2. La virtualización de la frontera durante el mandato de Nixon

La primera medida concreta para combatir el contrabando de drogas de México a EE.UU. la tomó el presidente Richard Nixon en 1969 con la Operación Intercepción. Según Grillo (2013), esta operación consistía en registrar "todo vehículo o peatón que cruzara la frontera sur mientras el ejército instalaba unidades móviles de radar entre los puestos" (p.

256). Este plan resultó un fiasco ya que pronto se hizo evidente que llevar a cabo un control terrestre tan exhaustivo era una utopía. El personal en tierra por sí solo simplemente no era capaz de sellar toda la frontera con México. Como observó Ghaffaray (2019), la frontera que separaba Estados Unidos de México era demasiado amplia y su orografía demasiado injustificada para ser cercada en su totalidad. Por esta razón, la Operación Intercepción, que costó 30 millones de dólares, solo duró 17 días.

No obstante, Mendoza (2023) destacó que Nixon se propuso fortificar la frontera mediante una valla virtual, no material, para lograr mejores resultados en la disminución de los flujos de drogas. Es decir, tras notar que el cierre físico de la frontera por sí solo era quijotesco, Nixon invirtió en la estructura de control de la frontera ya existente para mejorar la securitización de la misma tecnológicamente hablando. Además, Koslowski (2019) explicó en que en aquella época el gobierno estadounidense desplegó sensores de movimiento, infrarrojos, sísmicos y magnéticos que eran capaces de detectar tanto el movimiento como el calor desde un rango de 50 a 250 pies. La justificación que Nixon utilizó para legitimar la inversión en mecanismos digitales iba en la línea de proteger la frontera compartida con México: la Guerra contra las Drogas.

La necesidad de Nixon coincidía con los intereses de las empresas de alta tecnología militar de EEUU. El inminente final de la guerra de Vietnam obligó a estas empresas a diversificarse y a empezar a invertir en los sistemas de apoyo al ejército estadounidense. Para ello, tuvieron que convencer al Gobierno estadounidense de que siguiera invirtiendo en diferentes tipos de gasto militar, es decir, en una defensa que debía llevarse a cabo a nivel nacional en lugar de únicamente a nivel internacional. De ahí que, a partir de finales de los años sesenta, varias empresas de investigación y desarrollo contratadas por Estados Unidos para apoyar la intervención militar en Vietnam consiguieran firmar contratos federales.

Sylvania Electronics, por ejemplo, lo consiguió. Más concretamente, vendió en 1970 al gobierno estadounidense sus sensores terrestres utilizados para detectar a distancia movimientos sobre el terreno. Este fue un acontecimiento pionero, ya que simbolizó la primera aplicación de tecnologías virtuales utilizadas para vigilar la frontera sur de Estados Unidos. Grandin (2019) especificó que estos sensores se industrializaron como parte del plan del Secretario de Defensa Robert McNamara para construir una valla material y virtual que separara el norte del sur de Vietnam y se utilizaron para detectar los movimientos de tropas y camiones en la Ruta Ho Chi Minh. La función principal de estos sensores era percibir las actividades sísmicas provocadas por personas o camiones que pasaban cerca de los sensores y movían el suelo (Rosenau, 2001, pp. 11-12). Esta tecnología también era útil para detectar movimientos a través y en las proximidades de la frontera estadounidense; razón por la cual se implantó durante el mandato de Nixon.

Otro elemento tecnológico utilizado por primera vez durante la guerra de Vietnam y posteriormente en la frontera entre Estados Unidos y México fueron los drones. Estos drones, según Novak (2015), se conocían como RPV (Vehículos Pilotados a Distancia) -mientras que hoy en día se conocen como Vehículos Aéreos No Tripulados (UAV)- y se utilizaban para escanear la zona desde arriba. Al describir la frontera mexicana de 1972, Novak explicó que:

Los aviones sin piloto y teledirigidos *QU-22b* de la Fuerza Aérea estadounidense -que sobraban en Vietnam gracias a la introducción de drones más sofisticados- han sido

devueltos a Estados Unidos, donde [volaron] sobre la frontera para supervisar los sensores y retransmitir datos a los puntos de control centrales (Novak, 2015).

Con la llegada de los drones, se creó un centro de vigilancia que recibía la información recogida por los vehículos aéreos no tripulados. Barkan (1972, p. 1) racionalizó que estos vehículos aéreos no tripulados sobrevolaban tramos remotos de la frontera para retransmitir señales de cientos de sensores terrestres que luego se enviaban al llamado Centro de Vigilancia de Infiltración, donde enormes ordenadores diagnosticaban los datos.

5.2 Resultados y efectos aplicados de la titulización de Nixon

La guerra de Vietnam representa un hito para la securitización virtual de la frontera entre Estados Unidos y México bajo la presidencia de Nixon. De hecho, se produjo un claro cambio en la aplicación de tecnologías bélicas a las fronteras interiores de Estados Unidos, que se tradujo en una virtualización de la frontera. Estas novedades resultaron útiles a la Administración Nixon para alimentar el deseo de emprender la Guerra contra las Drogas. En consecuencia, todo esto vino acompañado de una participación política cada vez más decidida a sellar la frontera ( ), un término que normalmente se utiliza en misiones militares pero que por primera vez se relacionaba con la frontera estadounidense en aquella época (Lee, 2005), ya que uno de los objetivos principales era detener a los narcotraficantes que entraban por la frontera sur de Estados Unidos.

Aunque los sistemas de vigilancia introducidos por la Administración de Nixon no siempre funcionaron -como Barkan (1972, p. 2) señaló implacablemente, "no son capaces de distinguir entre amigos y enemigos"-, es innegable que constituyeron un paso importante en el control fronterizo estadounidense. Esta innovación resultó ser una piedra angular para casi todos los presidentes que le siguieron en lo que respecta a la gestión de la frontera sur de EEUU. El hecho de que una nueva tendencia tan importante se basara en un acto performativo, tal y como lo describe la teoría de la securitización, explica la importancia que tiene la creación de amenazas a la seguridad en la percepción del público a la hora de promover medidas de seguridad.

Tal y como se había debatido décadas después de la Guerra contra las Drogas, en realidad no existía tal cosa como una amenaza de las drogas, o al menos no en la medida en que el presidente Nixon remarcó en un principio. John Ehrlichman, el entonces Asistente del Presidente para Asuntos Internos bajo la presidencia de Nixon, admitió que la Administración mentía con respecto a la amenaza de las drogas para posibilitar movimientos políticos y militares (véase López, 2016). En todo caso, existía un verdadero problema de drogas entre los ejércitos estadounidenses en el extranjero y lejos del territorio estadounidense (véase Vulliamy, 2011).

La adopción de un enfoque de la frontera entre EE.UU. y México basado en la seguridad, tal como se inició bajo el mandato de Nixon, tiene consecuencias relacionadas. Es necesario considerar la literatura sobre el uso de alegorías como medios de polarización. Éstas, de hecho, dilucidan la relación que existe entre la securitización, los actos de habla y la creación de luchas sociales dentro del proceso más amplio de justificación de la vigilancia fronteriza y los poderes de emergencia. Este es el caso de Kruglanski (2007), que se centró en la idea de las metáforas para ilustrar de qué manera el lenguaje es capaz de enmarcar las amenazas determinando el proceso de respuesta

política. El discurso de Nixon centrado en el "enemigo número uno" coincide con la metáfora bélica de Kruglanski. Para ser más precisos, las metáforas bélicas de Nixon reflejan las del discurso sobre el terrorismo propuestas por Kruglanski (2007). Esto indica que la securitización de la frontera estadounidense se ha utilizado incluso en épocas más recientes. En ambos casos, la respuesta totalizadora fue posible gracias a la legitimación de medidas de emergencia como la vigilancia fronteriza.

Las desventajas de utilizar un enfoque de este tipo en el proceso de securitización de EE.UU. se encuentran en los efectos polarizadores y radicalizadores que tienen a largo plazo. Por ejemplo, Moyano *et al.* (2016) criticaron el proceso de securitización de la era Bush (la Guerra contra el Terror) causado por el acto terrorista del 11 de septiembre. En su opinión, la sociedad estadounidense se habría beneficiado más de una narrativa menos polarizadora que evitara las disyunciones sociales que afectan a la división social actual. Lo mismo puede decirse del enfoque de Nixon con respecto a la Guerra contra las Drogas. De hecho, siguiendo esta idea, enmarcar la cuestión como una guerra en lugar de como un desafío humano eclipsó los problemas asociados de salud pública y desarrollo comunitario que aquejaban a Estados Unidos. Hubiera sido aconsejable, por tanto, adaptar la concepción de sus actos discursivos. A la larga, habría sido más rentable optar por una respuesta más holística. Éstas deberían haberse basado en un enfoque multidisciplinar para evitar los contragolpes creados por los procesos de securitización que sólo tienen en cuenta una cuestión.

6. DEBATE

Este documento se dedicó a buscar una respuesta a las siguientes preguntas de investigación: ¿Cómo contribuyó la Guerra contra las Drogas bajo la Administración Nixon a la transición de un control fronterizo físico a lo largo de la frontera sur a mecanismos de aplicación de la ley virtuales? Para encontrar una respuesta a esta pregunta, esta investigación hizo uso de los principales principios que componen la teoría de la securitización. Estos principios se utilizaron como indicadores para llevar a cabo un análisis del discurso de dos discursos pronunciados por Nixon en los que declaraba oficialmente su Guerra contra las Drogas. Lo que resultó de este análisis es que el presidente Nixon participó activamente en el encuadre de una amenaza a la seguridad propuesta a su audiencia pública y política como perjudicial para la seguridad nacional de todo el país. Gracias a la aceptación por parte de la audiencia de la narrativa dada, se adoptaron medidas extraordinarias para detener la entrada de drogas en los Estados. Entre estas medidas fue posible identificar la introducción de mecanismos virtuales de represión.

Investigaciones anteriores han señalado la importancia que ha tenido la frontera virtual en la definición de la frontera sur de Estados Unidos. Heyman (2008) destacó cómo los muros y las vallas se ven reforzados por el aspecto virtual que define el lado coercitivo de la política de inmigración estadounidense. Una idea que avanzaron Amoore *et al.* (2008, pp. 99-100) al enumerar el conjunto de tecnologías utilizadas para ayudar a la Patrulla Fronteriza estadounidense a clasificar mediante algoritmos lo que puede considerarse una amenaza y lo que no. Así pues, su estudio se centraba en el cambio del papel humano en la gestión de las fronteras junto con la capacidad de control de EE.UU. más allá de la frontera física gracias al aspecto virtual de su límite. Otro tipo de investigación realizada sobre la virtualización de la frontera estadounidense estuvo vinculada al desarrollo militar. Como sugirió Adams (2001), los avances militares en el

uso de la tecnología para llevar a cabo la guerra se utilizaron para revigorizar la frontera inteligente que separa EE.UU. de México con el fin de garantizar una supervisión óptima.

Teniendo en cuenta esta investigación existente, se puso de manifiesto una laguna en la bibliografía. Es decir, aunque se ha estudiado la securitización, virtualización y militarización fronteriza a lo largo de la frontera sur de Estados Unidos, no se ha considerado adecuadamente el inicio de esta transformación. Lo que este documento pretendía era precisamente llenar este vacío. Tras llevar a cabo esta investigación, se hizo evidente que la presidencia de Nixon resultó ser pionera para la historia de la gestión de fronteras en Estados Unidos. De hecho, fue la primera vez que los Estados implementaron elementos tecnológicos -como sensores en tierra y las primeras versiones de vehículos aéreos no tripulados- para vigilar la frontera entre EE.UU. y México. Al colmar esta laguna presente en el debate académico sobre los orígenes de la frontera inteligente de los Estados, es posible seguir impulsando la investigación y la comparación de las fronteras desde la perspectiva de los estudios de seguridad. Además, al poner a prueba la teoría de la securitización para llevar a cabo con éxito un análisis del discurso emprendido por las élites políticas para enmarcar las necesidades de seguridad, las conclusiones de esta investigación pueden aplicarse también a otros casos. Por ejemplo, sería posible aplicar esta investigación a casos similares como el de la frontera española compartida con Marruecos. La teoría de la securitización utilizada como en el presente estudio podría arrojar luz sobre cómo y cuándo se introdujeron los mecanismos de fronteras virtuales en el régimen fronterizo español.

No obstante, es necesario mencionar también las limitaciones de este trabajo. Aunque la elección de realizar un estudio de caso único era necesaria para ofrecer una descripción precisa del papel de Nixon en el fomento de la virtualización de la frontera entre EE.UU. y México, un estudio comparativo podría haber ofrecido una comprensión global de las fronteras en general. Del mismo modo, la utilización de un método mixto para llevar a cabo este estudio también podría aumentar la validez de las conclusiones . La integración de una perspectiva cuantitativa en el enfoque cualitativo favorecido en esta investigación podría aportar información importante a la hora de localizar qué partes de las fronteras se fortificaron más en relación con el proceso de virtualización.

Las limitaciones de este trabajo representan, no obstante, una oportunidad para estimular nuevas investigaciones sobre este tema. La comparación de las conclusiones de este estudio con otros casos en los que se han producido importantes avances en la virtualización de las fronteras como parte de un proceso de fortificación más general. Las ciudades autónomas españolas de Ceuta y Melilla, por ejemplo, podrían beneficiarse de este tipo de análisis. Comprender su proceso de fortificación fronteriza a partir de su adhesión al Espacio Schengen aportaría datos significativos sobre cómo ha cambiado la gestión de las fronteras debido a las prácticas fronterizas virtuales. Establecer si el inicio de esta digitalización se complementó con el ejemplo proporcionado anteriormente por EE.UU. podría ayudar a concebir las fronteras de Ceuta y Melilla de una forma más completa. Además, emparejar la teoría de la securitización a estos casos concretos podría desvelar la doble importancia de la narrativa nacional que justifica este cambio en el régimen fronterizo junto con la narrativa implementada por la Unión Europea. De este modo, sería posible analizar la idea de la Fortaleza Europa desde el punto de vista de la securitización virtual.

En general, los intentos de Nixon de contrarrestar el contrabando de drogas a través de la frontera sur de EE.UU. sentaron las bases de décadas de política fronteriza entre EE.UU. y México. La importancia de este cambio en el régimen fronterizo es visible en el actual *modus operandi* de la Patrulla Fronteriza. Mantener el control de la frontera sur sería prácticamente imposible sin las tecnologías militares estadounidenses utilizadas en Vietnam e introducidas en la frontera nacional bajo Nixon. Al rastrear los orígenes del control fronterizo virtual hasta la Guerra contra las Drogas de Nixon, este estudio revela cómo la política de seguridad puede transformar silenciosamente la arquitectura misma de las fronteras de una nación.

REFERENCIAS BIBLIOGRÁFICAS

Adams, J. (2001). Defensa virtual. *Foreign Affairs*, *80*(3), 98-112.

Amoore, L., Marmura, S., & Salter, M. B. (2008). Fronteras inteligentes y movilidades: Espacios zonas, enclosures. *Surveillance & Society*, *5*(2).

Armstrong, W. G. (1992). Punishment, Surveillance, and Discipline in Paradise Lost. *Studies in English Literature, 1500-1900*, *32*(1), 91-109. https://doi.org/10.2307/450942

Barkan, R. (1972, 18 de febrero). Te observan, a través de las paredes, en la oscuridad de la noche mientras caminas, y viene de vietnam. *Free Press*.

Dafoe, A. (2015). Sobre el determinismo tecnológico: Una tipología, condiciones de alcance y un Mechanism. *Ciencia, tecnología y valores humanos*, *40*(6), 1047-1076. http://www.jstor.org/stable/43671266

Ghaffary, S. (2019, 16 de mayo). El muro "más inteligente": Cómo drones, sensores y ai están patrullando la frontera. Vox.

Grandin, G. (2019, 9 de febrero). Cómo Estados Unidos armó el muro fronterizo. The Intercept.

Grillo, I. (2013). Los cárteles mexicanos: Un Siglo Desafiando la Política Antidrogas de Estados Unidos. The Brown Journal of World Affairs, 20(1), 253-265. http://www.jstor.org/stable/24590897

Heyman, J. McC. (2008). Constructing a Virtual Wall: Race and Citizenship in U.S.-Mexico Border Policing. *Journal of the Southwest*, *50*(3), 305-333.

Kerr, D. (1999). Decapitar al rey y entronizar el mercado: A Critique of Foucauldian Governmentality. *Science & Society*, *63*(2), 173-202.

Koslowski, R. K. (2019, 29 de mayo). *Las reformas de la inmigración y la seguridad fronteriza fronteras*. Artículos. https://items.ssrc.org/border-battles/immigration-reforms -y-las-tecnologías-de-seguridad-fronteriza/

Kruglanski, A. W., Crenshaw, M., Post, J. M., & Victoroff, J. (2007). What Should This Fight Be Called? Metaphors of Counterterrorism and Their Implications. *Psychological Science in the Public* Interest, *8*(3), 97-133. http://www.jstor.org/stable/40062365

Lee, J. (2005, 31 de agosto). James H. Scheuer, 13-term New York congressman, is dead a los 85 años. The New York Times.

Lemke, T. (2015). *Foucault, gubernamentalidad y crítica*. Routledge.

López, G. (2016, 22 de marzo). *Funcionario de Nixon: La verdadera razón de la guerra contra las drogas fue criminalizar a los negros y a los hippies.* Vox. https://www.vox.com/2016/3/22/11278760/war-on- drogas-racismo-nixon

Lynch, M. (2008). *Ideas y perspectivas.* En *The Handbook of Socience and Technology Studies* editado por Hackett, E. J., Amsterdamska, O., y Wajcman, J., 9-11. Cambridge, MA: MIT Press

Mendoza, M. E. (2023, 30 de octubre). *La historia del muro fronterizo entre Estados Unidos y México*. Time. https://time.com/6324599/bidens-trump-history-border-wall/

Moyano, M., Bermúdez, M. I. ., & Ramírez, A. (2016). Psicología positiva para afrontar la radicalización y el terrorismo? Un análisis del discurso de Obama en el Cairo. *Escritos De Psicología - Psychological Writings*, *9*(3), 53-58. https://doi.org/10.24310/espsiescpsi.v9i3.13219

Nail, T. (2016). *Teoría de la frontera*. Oxford University Press.

Novak, M. (2015, 24 de septiembre). Cómo la guerra de Vietnam trajo la vigilancia de alta tecnología a Estados Unidos. Gizmodo.

Otukoya, T. A. (2024). The securitization theory. *Revista Internacional de Ciencia e Investigación*, *11*(1), 1747-1755. https://doi.org/10.30574/ijsra.2024.11.1.0225

Paden, R. (1984). Vigilancia y tortura: Foucault and Orwell on the Methods of disciplina. *Teoría y práctica social*, *10*(3), 261-271.

Reid, Justin M. "'An Exercise in International Extortion': Operation 'Intercept' and Nixon's 1969 War on Drugs". Tesis de máster, Chapman University, 2022. https://doi.org/10.36837/chapman.000412

Sharma, V. (2023). Una revisión de la "Teoría de la frontera" de Thomas Nail. Nueva Zelanda Revista de Estudios Asiáticos.

Smith, M. R., & Marx, L. (Eds.). (1994). *¿Impulsa la tecnología la historia? El dilema del determinismo tecnológico*. Mit Press.

Timmons, P. (2017). El muro de Trump en la frontera de Nixon: Cómo la Operación Intercept sentó las bases de décadas de política fronteriza entre Estados Unidos y México, incluido el muro de Donald Trump. *NACLA Informe sobre las Américas, 49*(1), 15-24. https://doi.org/10.1080/10714839.2017.1298238

Toshkov, D. (2016). Diseño de investigación en ciencia política. Basingstoke: Palgrave Macmillan.

Trist, N., Cuevas, L., Couto, B., & Atristain, M. (2022). El Tratado de Guadalupe Hidalgo. En G. M. Joseph & T. J. Henderson (Eds.), *The Mexico Reader: History, Culture, Politics* (pp. 599-603). Duke University Press. https://doi.org/10.2307/j.ctv2rr3g8m.96

Aduanas y protección de fronteras de los Estados Unidos. (2019). *Sabías que... Obeliscos centenarios marcan Línea fronteriza entre México y Estados Unidos?*. Aduanas y protección fronteriza de Estados Unidos. https://www.cbp.gov/about/history/did-you-know/obelisk

Departamento de Defensa de los Estados Unidos (2017). *41 Nixon Remarks Intensified Program for Drug Abuse*. Gobierno de EEUU.

Vulliamy, E. (2011, 23 de julio). *La "Guerra contra las Drogas" de Nixon comenzó hace 40 años, y la batalla batalla sigue abierta*. The Guardian. https://www.theguardian.com/society/2011/jul/24/war-on- drogas-40-años

Wæver, O. (1995). Securitization and Desecuritization. En R. D. Lipschutz (Ed.), *On Security* (pp. 46-87). Columbia University Press.

Revista Científica del Centro Universitario de la Guardia Civil
Revista Lógos Guardia Civil

Artículo de Investigación

VIOLENCIA SEXUAL EJERCIDA POR DESCONOCIDOS EN MADRID Y BARCELONA: UN ANÁLISIS SITUACIONAL

Francisco Pérez Fernández
Doctor en Filosofía y Ciencias de la Educación, Profesor Contratado Doctor (Psicología Criminal, Psicología de la Personalidad e Historia de la Psicología), Departamentos de Psicología y de Criminología y Seguridad, Facultad HM Hospitales de Ciencias de la Salud, Universidad Camilo José Cela
fperez@ucjc.edu
ORCID ID: 0000-0002-3039-2397
Google Scholar: https://scholar.google.es/citations?hl=es&user=O_7qrwgAAAAJ

Heriberto Janosch
Doctor en Ciencias Jurídicas y Económicas,
Profesor de Historia de la Psicología y de Bases Biológicas del Comportamiento, Facultad de Salud, UNIE Universidad
heriberto.janosch@universidadunie.com
ORCID ID: 0000-0002-0188-2434
Google Scholar: https://scholar.google.com/citations?user=uA4iKy0AAAAJ

Enrique López López
Magistrado de la Audiencia Nacional de España.
Profesor de Derecho Constitucional y de Derecho Procesal Penal, Facultad de Ciencias Jurídicas y Relaciones Internacionales, UNIE Universidad
enrique.lopezl@universidadunie.com

Francisco López-Muñoz
Doctor en Medicina y Cirugía y Doctor en Lengua Española y Literatura, Catedrático de Farmacología y Vicerrector de Investigación y Ciencia, Facultad HM Hospitales de Ciencias de la Salud, Universidad Camilo José Cela
flopez@ucjc.edu
ORCID ID: 0000-0002-5188-6038
Google Scholar: https://scholar.google.es/citations?user=IbuwtWgAAAAJ&hl=es

Recibido 28/03/2025
Aceptado 23/05/2025
Publicado 27/06/2025

Cita recomendada: Pérez, F, Janosch, H, López, E y López, F (2025). Violencia sexual ejercida por desconocidos en Madrid y Barcelona: un análisis situacional. *Revista Logos Guardia Civil*, 3(2), p.p. 171-196.

Licencia: Este artículo se publica bajo la licencia Creative Commons Atribución-NoComercial-SinDerivadas 4.0 Internacional (CC BY-NC-ND 4.0)
Depósito Legal: M-3619-2023
NIPO en línea: 126-23-019-8
ISSN en línea: 2952-394X

VIOLENCIA SEXUAL EJERCIDA POR DESCONOCIDOS EN MADRID Y BARCELONA: UN ANÁLISIS SITUACIONAL

Sumario: 1. INTRODUCCIÓN. 2. HIPÓTESIS. 3. METODOLOGÍA. 4. RESULTADOS. 5. DISCUSIÓN. 6. CONCLUSIONES. 7. REFERENCIAS BIBLIOGRÁFICAS.

Resumen: Las agresiones sexuales, en tanto que delitos de especial significación victimal y mediática, suscitan gran alarma, preocupación e interés públicos. En consecuencia, suelen formar parte del epicentro del debate general en torno a las políticas criminales. Ello motiva que las agresiones sexuales y sus protagonistas -agresor y víctima- no siempre sean adecuadamente analizados, tratados y entendidos fuera de los entornos criminológicos, policiales y jurídicos. Del mismo modo, la propia investigación criminológica, así como el devenir legislativo, jurídico y penitenciario vinculados al tema -necesariamente controvertido-, tienden a menudo a difuminarse en generalidades teóricas que cuesta confrontar e incluso encajar con hechos y casos particulares que, al estudiarse en detalle, parece imposible de encajar en los marcos explicativos generales de que se dispone. El presente estudio, que se realiza partiendo del enfoque aportado por la Teoría de la Acción Situacional (TAS), propuesta por Wikström y sus colaborares, y se vale del análisis cualitativo y cuantitativo de sentencias judiciales emitidas en las provincias de Madrid y Barcelona, pretende mostrar cómo los ecosistemas criminales en que se cometen los delitos, modifican sustancialmente su curso, así como las acciones del agresor y su víctima. Un hecho que puede ser extremadamente útil como herramienta para la investigación policial y el análisis de conducta, así como para la comprensión de eventos criminogenéticos y dinámicas criminales específicas.

Abstract: Sexual assaults, as crimes of special impact and media significance, arouse great public alarm, concern, and interest. Consequently, they are often at the center of the general debate surrounding criminal policies. This means that sexual assaults and its actors -offenders and victims- are not always well analyzed, addressed, and understood outside of criminological, police, and legal circles. Similarly, criminological research itself, as well as the legislative, legal, and penitentiary developments linked to the necessarily controversial topic, often tend to be blurred into theoretical generalities that are difficult to compare and even reconcile with particular facts and cases that, when studied in detail, seem impossible to fit into the general explanatory frameworks available. This study, based on the approach provided by the Situational Action Theory (TAS) proposed by Wikström and colleagues, and focused on the qualitative and quantitative analysis of court rulings issued in the provinces of Madrid and Barcelona, aims to show how the criminal ecosystems in which crimes are committed, substantially modify their course, as well as the actions of offender and their victim. This fact can be extremely useful as a tool for police investigation and behavioral analysis, as well as for understanding criminogenic events and specific criminal dynamics.

Palabras clave: Agresión Sexual, Teoría de la Acción Situacional, Escalamiento Multidimensional, Análisis de Conducta.

Keywords: Sexual Assault, Situational Action Theory; Multidimensional Scaling, Behavior Analysis.

1. INTRODUCCIÓN

Las agresiones sexuales son una fuente de sufrimiento para las víctimas. Hecho agravado en aquellos casos que, por razones peculiares, se hacen especialmente "famosos" y concitan el interés de la opinión pública. El hecho es que las agresiones sexuales, a menudo muy publicitadas, provocan gran alarma y debate social, lo cual suele desencadenar investigaciones y juicios particularmente mediáticos que suscitan un fuerte impacto en las víctimas por la vía de la victimización secundaria y *ex post attendentes*[1] (Gutiérrez de Piñeres, Coronel y Pérez, 2009; Domínguez Vela, 2016). Por aportar algún dato para la reflexión, se recordará que, según el Anuario Estadístico del Ministerio del Interior de España, en 2022 se "conocieron" por parte de las Fuerzas y Cuerpos de Seguridad del Estado (FCSE) -se habla de denuncias e investigaciones- 19.013 delitos contra la libertad sexual, de los cuales 11.426 fueron abusos/agresiones sexuales y, de entre ellas, 4.270 se convirtieron en abusos/agresiones sexuales con penetración[2]. Un elevado porcentaje de estas agresiones/abusos se tuvieron lugar en locales comerciales, viviendas y otros espacios anexos tales como garajes o trasteros, siendo una de las modalidades más frecuentes de esta tipología de crímenes aquella en la que el agresor sexual, habitualmente un varón que actúa en solitario, ataca a una mujer en el portal de acceso a un edificio de viviendas, o bien en el garaje, por lo cual recibe la denominación común de "portalero" (Janosch González, Pérez-Fernández y Soto Castro, 2020).

Sea como fuere, la "cifra gris" que se observa en la estadística refleja que en el fondo de este problema subyace una evidencia policial, victimal y judicial ominosa: el esclarecimiento de las agresiones sexuales cometidas por individuos desconocidos para las víctimas es más complejo que el de aquellos casos en las que existe algún tipo de vínculo entre víctima y victimario que facilite a los investigadores de las FCSE una identificación positiva del agresor y la consiguiente obtención, llegado el caso, de indicios que puedan obrar como prueba en sede judicial (Corovic, Christianson y Bergman, 2012; Janosch, Pérez-Fernández y Herrero, 2025). Téngase en cuenta, al hilo de lo expuesto, que la dinámica cognitivo-conductual de estos individuos tiende a operar mediante un proceso de escalada, lo cual implica que, con relación con su potencial peligrosidad, es muy posible la presencia de un sesgo de serialidad -o cuando menos repetitividad- que los conduzca a cometer más de una agresión sexual en el transcurso de su carrera delictiva en el caso de no ser identificados y detenidos (Pueyo y Redondo Illescas, 2007). Especialmente porque, antes que un vínculo directo con trastornos diagnosticables más o menos graves, en esta clase de agresores parece verse impulsada por la influencia de una amalgama compleja de elementos socioculturales, estresores vitales y estructuraciones de la personalidad (Arqué-Valle et al., 2024).

---

[1] A menudo se confunden ambos tipos de victimización. La secundaria se relaciona con los costes personales y psicológicos que tiene para la víctima el hecho de estar expuesta de manera más o menos constante a situaciones que la hacen revivir (o rememorar) el daño sufrido una y otra vez (Kühne, 1986). La victimización *ex post attendentes* -también llamada "de cuarto nivel"- se desencadena cuando la persona experimenta desesperanza y desamparo tras no recibir la ayuda esperada por parte de aquellas instituciones y profesionales en los que confiaba (como cuerpos policiales, sanidad, administración, justicia) y de los que no recibe el apoyo moral y material esperado (Triviño, Winberg y Moral, 2021).

[2] En total se esclarecieron, contando todas las tipologías de delitos contra la libertad sexual, un total de 14.555, lo cual arroja un montane de "cifra gris" -delito investigado, pero no aclarado- de 4.518 denuncias. En lo tocante a abusos/agresiones con penetración, las no esclarecidas en el año 2022 fueron 860 (Ministerio del Interior, 2023).

Por otro lado, y abundando en la última idea, es bien conocido que el contexto -ambiente material y humano- en el que el delincuente actúa modifica su comportamiento, por lo que las estrategias y recursos que pueden ser perfectamente útiles en determinado lugar no necesariamente tienen por qué tener el mismo valor de aplicabilidad en otro ecosistema criminal-delincuencial diferente. Wikström, enfrentado a esta contingencia, desarrolló la así llamada Teoría de la Acción Situacional de las Causas del Crimen (o TAS), cuyas propuestas fundacionales aparecieron entre 2004 y 2006 (Serrano Maíllo, 2017). Allí se ha intentado integrar, dentro del marco de una teoría adecuada de la acción, los principales logros de las formulaciones teóricas e investigaciones de la criminología, además de los conocimientos teóricos y empíricos de las ciencias sociales y del comportamiento en general. Y ello porque se conocen bastante bien los correlatos de la criminalidad, pero hay poco acuerdo acerca de cuáles son sus causas, que se ofrecen como una mezcla confusa de elementos a los que cada investigador concede mayor o menor importancia en función de sus intereses. Así se explica la inflación de teorías -y contradicciones internas- que afectan a los estudios criminológicos (Pérez-Fernández, Janosch y Popiuc, 2023).

Resumiendo, la TAS establece que se pueden explicar los actos delictivos como procesos -mecanismos sistémicos e interactivos, pero no determinísticos- que movilizan "acciones" que, en última instancia, transgreden reglas formales o informales de conducta (Wikström, et al., 2012). Se trataría por lo tanto de un subconjunto de conductas incluido en el conjunto más general de *actos que violan reglas de conducta morales*. Aunque estos constructos de conducta moral no están especificados en ley alguna y, por lo tanto, no todos ellos son delitos por sí mismos, sí podrían responder a los mismos mecanismos que movilizan los delitos en un sentido legal (Janosch González, 2013). De otro modo: la TAS define el crimen como un acto que quebranta alguna regla de conducta establecida en la ley -inserta en el código penal de cada estado-, y que puede ser analizado en términos de *acción moral*. Ésta, por su parte, se entendería como aquella conducta que está guiada por reglas que establecen qué es lo que, bajo determinadas circunstancias concretas -o situaciones-, estaría bien o mal hacer (Wikström y Treiber, 2016).

Definir el delito en estos términos, como un acto que viola una regla de conducta moral que se plasma en la forma de leyes, tiene la ventaja de que puede aplicarse a cualquier tipo de delito, en cualquier lugar, y en cualquier época. Así, lo que se define es un acto de violación de una regla de conducta moral que se especifica en la forma de alguna ley concreta "ahí dada". Puede por ello afirmarse que la TAS es, fundamentalmente, una teoría general de la acción moral (Wikström, et al., 2012), ya que explicaría todos los tipos de quebrantamiento de las reglas morales en cualquier tiempo o lugar, haciendo hincapié en el mecanismo que induce a dicho quebrantamiento, y no en el contenido de la regla moral desobedecida en tanto que variable y sometido a modificaciones constantes en función de las variaciones del derecho positivo concreto en un espacio-tiempo específico (Pauwels, 2018a; Pauwels, 2018b). El mecanismo causal de percepción y acción estaría presente tanto en pequeños hurtos como en agresiones sexuales u homicidios. Consecuencia: las políticas criminales, a medio y largo plazo, tendrían más éxito si se destinaran a la educación en conformidad con la regla moral vigente, que hacia la sanción o el mero control (Pérez-Fernández, Janosch y Popiuc, 2023; Janosch, Pérez-Fernández, Popiuc y López-Muñoz, 2024).

En última instancia, la interacción entre la propensión al delito que tenga una persona en concreto, y las características criminogénicas del escenario, son lo que

desencadenará el proceso que llevará -o no- al acto criminal en sí. La propensión al delito dependerá de las normas morales de la persona y de su capacidad de ejercer autocontrol -teniendo en cuenta que esta capacidad puede estar disminuida por consumo de alcohol o drogas, o por un estrés intenso con desequilibrio emocional-. Dichas características criminogénicas del escenario, a su vez, dependerán de la llamada "moral del ambiente" -la percibida por el individuo antes que la real- y de la existencia o no de factores disuasorios, que alienten o no la violación de las normas (Wikström, et al., 2012). El corolario de todo esto, en lo que este estudio respecta, es claro: el agresor sexual no actuará siempre igual y con total independencia del lugar en que se encuentre, pues la situación general en la que se inserte -que ha de ser analizada y comprendida- va a modificar necesariamente su percepción de reglas, sus consideraciones morales, su atención a leyes y restricciones y, por último, a su acción delincuencial (Pérez-Fernández, Popiuc y López-Muñoz, 2024).

Consideradas las cosas de este modo se entenderá que, para la TAS, más allá de ideas opinables, la nacionalidad, la ideología política, la identificación sexual o la religión de una persona, no son causas por sí mismas de la delincuencia en ninguna de sus formas o, cuando menos, no debieran evaluarse como más importantes que otras circunstancias personales, tales como la edad o el nivel de estudios, pues en realidad se trata de meros atributos de la persona que, por lo demás, son cambiantes. Del mismo modo que no tendría sentido decir que alguien es más propenso a cometer delitos por tener mayor estatura, tampoco lo tiene hacer hincapié en otros atributos personales que, además, entrarían en el controvertido ámbito de los derechos y libertades individuales. Así, se deben evaluar variables como la nacionalidad o la religión con el mismo rigor que otras concausas coadyuvantes a diferentes formas de delincuencia reconocidas en la literatura, tales como la pobreza, el nivel de estudios, vivir en ambientes criminógenos, la falta de oportunidades, los policonsumos, el absentismo escolar, las compañías inadecuadas y etcétera (Pérez-Fernández, Janosch y Popiuc, 2023). Dicho de otra manera: al igual que carecería de sentido afirmar que una persona comete delitos -o no lo hace- a causa del color de su cabello o de su peso en kilogramos, tampoco es coherente sostener que podría verse impelida a cometerlos por el mero hecho de haber nacido en determinado país, de ser partícipe de determinado sentir ideológico, de identificarse con un género específico o de practicar determinada religión (Janosch, Pérez-Fernández y Herrero Roldán, 2024).

1.1. UN NECESARIO APUNTE JURÍDICO

Se concluye esta introducción recordando algo sobradamente conocido, y es que en España ha habido cambios relativamente recientes en el Código Penal (CP) con respecto a los delitos de carácter sexual, que han venido a modificar las diferentes perspectivas existentes en lo tocante al abordaje policial y judicial del problema. Para empezar, y enlazando con el modelo TAS descrito anteriormente, suponen una alteración de los contajes estadísticos -lo que también alterará discursos mediáticos futuros- cuyos efectos solo serán perceptibles a medio plazo y, en consecuencia, abren nuevas panorámicas de percepción general de la criminalidad, así como de políticas reactivas de actuación con respecto a ella cuyos efectos están por llegar. Merece la pena, pues, a fin de anticipar lo que viene y de cara a contextualizar adecuadamente los resultados que aquí se ofrecen, aportar una breve reseña crítica de tales modificaciones.

La LO 10/2022, de 6 de septiembre, conocida popularmente como la *Ley del solo sí es sí*, ha supuesto un notable cambio con respecto a la consideración de los delitos

contra la libertad sexual. Esta normativa ha introducido cambios significativos en el CP, especialmente en la unificación de los delitos de abuso y agresión sexual, la redefinición del consentimiento y la modificación de las penas asociadas. Pero, al margen de estas novedades legislativas, ha generado también un intenso debate como consecuencia de las rebajas de penas que se han producido: 1205 reducciones de pena que incluyen 121 excarcelaciones (CGPJ, 2023). La promulgación de esta ley se contextualizó en la necesidad de reforzar la protección de la libertad sexual y garantizar una respuesta integral frente a todas las formas de violencia sexual.

Previamente a la entrada en vigor de la LO 10/2022, el CP español distinguía entre abuso y agresión sexuales. El abuso se refería a actos sin violencia o intimidación, mientras que la agresión implicaba el uso de estas. Con la nueva ley, esta distinción desaparece. Así, cualquier acto sexual sin consentimiento se considera agresión sexual, independientemente de si hubo violencia o intimidación. Esta unificación busca reconocer que toda acción sexual no consentida es una agresión a la libertad sexual de la persona.

La ley establece que solo se entiende que hay consentimiento cuando este se haya manifestado libremente, mediante actos que, en atención a las circunstancias del caso, expresen de manera clara la voluntad de la persona. Esta definición coloca el consentimiento en el centro de las relaciones sexuales, eliminando interpretaciones que pudieran justificar conductas no consentidas. Ello implica que cualquier acto sexual no consentido es agresión, con independencia de que haya o no violencia o intimidación, porque la sola ausencia del consentimiento ya supone una violencia implícita. Aunque no se definiera explícitamente el consentimiento, ello no significaba que la jurisprudencia no entendiese que tal consentimiento era sustancial, como un elemento en este caso negativo del tipo, que el agente actuara: 1) sin consentimiento de la persona agredida sexualmente; 2) mediante la existencia de un consentimiento viciado por circunstancias concurrentes derivadas de la posición del autor del hecho, significativamente provenientes de parentesco o una situación equivalente, o bien del dominio que su posición consecuencia de una relación laboral, docente, de superioridad, de ascendencia, incluso consecuencia de un rango de edad con respecto a la víctima, pudiera coartar a ésta de su libre determinación sexual; y 3) que el agente se valiera de una posición de privilegio deducida de la vulnerabilidad de la víctima o de su estado de inconsciencia[3]. Estas últimas secuencias de ataques frente a la libertad sexual fueron catalogadas como abusos sexuales con anterioridad, mientras que los casos en que el autor actuaba contra el consentimiento de la víctima abrían la categoría de agresión sexual, siendo cometidos mediante violencia o intimidación, que era la característica que exigía tal agresión. No obstante, siempre fue necesaria la concurrencia de esa ausencia de consentimiento que impregna el título que abraza estos delitos, pues lo son contra la libertad sexual, que se basa naturalmente en la existencia de consentimiento en la prestación de este para llevar a cabo acciones con contenido sexual.

La fórmula que utiliza hoy el legislador es, pues, una fórmula abierta, y que ya se tomaba en consideración jurisprudencialmente, en términos similares, para entender concurrente el consentimiento. La referida fórmula descansa en actos, de modo que "sólo se entenderá que hay consentimiento cuando éste se haya manifestado libremente

3 Véase, por ejemplo: STS 3865/2024; SAP A 872/2018.

mediante actos que, en atención a las circunstancias del caso, expresen de manera clara la voluntad de la persona" (LO 10/2022). Por *actos*, se han de entender todo tipo de manifestaciones o señales de la persona que va a consentir, ya sean verbales, gestuales o situacionales, pero deben de ser considerados como explícitos. De modo que el consentimiento se construye como positivo y concluyente, y ha de ser libremente prestado (implícitamente, no viciado: debe depender exclusivamente de la voluntad de la persona, como en cualquier delito cuyo objeto genérico de protección es la libertad en cualquiera de sus expresiones).

La reforma motivada por la aprobación de la LO 10/2022 ha ajustado, también, las penas asociadas a los delitos sexuales. Por ejemplo, la agresión sexual sin penetración tenía anteriormente una pena de 1 a 5 años de prisión, mientras que con la nueva ley se establece una horquilla de 1 a 4 años. En el caso de agresiones con penetración, la pena mínima se reduce de 6 a 4 años, manteniendo el máximo en 12 años. Estas modificaciones han sido objeto de controversia, especialmente por el efecto de su aplicación retroactiva en beneficio de condenados. La aplicación retroactiva de la ley, principio básico del derecho penal cuando una norma favorece al reo, ha llevado a la revisión de numerosas sentencias firmes. Este efecto no previsto ha generado un intenso debate sobre la necesidad de ajustar la ley para evitar consecuencias no deseadas, algo que finalmente se hizo por LO 4/2023, de 27 de abril.

No cabe duda de que la Ley Orgánica 10/2022 estaba guiada por un objetivo loable en la protección de la libertad sexual al unificar delitos y centrar la atención en el consentimiento. No obstante, la reducción de penas en ciertos casos ha evidenciado la complejidad de reformar el CP, por lo que es fundamental que futuros cambios consideren detalladamente las implicaciones prácticas de las modificaciones legislativas para garantizar una protección efectiva de las víctimas y una adecuada sanción a los agresores. La controversia descrita ha venido al tocarse tanto los límites penales máximos como mínimos sin prever la posibilidad de introducir una disposición transitoria. El CP en una democracia es un instrumento extremadamente importante y debiera quedar al margen de ideologías y sectarismos.

2. HIPÓTESIS

Es cierto que la legislación a aplicar es la misma en Madrid y en Barcelona, siendo por otro lado idénticas las condiciones de aplicación de éstas, con lo cual el planteamiento legal de partida -y sus vicisitudes- serán básicamente el mismo. Sin embargo, si se presta atención al modelo TAS anteriormente descrito queda claro que, aceptando que el contexto en el que el delincuente potencial desarrolla sus actividades habría de modificar su comportamiento, se implica que las estrategias y recursos que pueden ser perfectamente útiles en la provincia de Madrid no necesariamente tienen por qué tener el mismo valor de aplicabilidad en otro ecosistema criminal-delincuencial diferente, como el de la provincia de Barcelona, en el que, además, se opera bajo el control de cuerpos policiales y modelos penitenciarios también diferenciados.

En consecuencia, el interés de este artículo se sustancia en la formulación y estudio de una hipótesis básica: Las agresiones sexuales perpetradas en la provincia de Madrid habrán de ser, de alguna manera y en tanto en cuanto que mediadas por modelos de acción situacional diferentes, significativamente diferentes de las agresiones sexuales cometidas en la provincia de Barcelona.

3. METODOLOGÍA

Es cierto que la investigación criminológica no encuentra en las diferentes bases de datos públicas de España datos suficientes o apropiados para someter a prueba sus planteamientos. El problema, ya criticado con profusión por otros investigadores, reside en que se trata de información recabada con propósitos público-administrativos que responden a las competencias del organismo competente, por lo que raramente tiene en cuenta las necesidades de las/los investigadoras/es y suele atender a otros criterios, no coherentes con las pretensiones de la ciencia (Linde y Aebi, 2021). Resulta singularmente excepcional, no obstante, la información que proporciona el Centro de Documentación Judicial (CENDOJ) del Consejo General del Poder Judicial (CGPJ), pues ofrece los datos sin filtrar, permitiendo a las/os investigadoras/es procesarlos para adaptarlos a sus necesidades específicas. No obstante, dadas otras carencias inherentes a la propia naturaleza de esta base de datos, la documentación que aporta debe categorizarse y filtrarse adecuadamente, a partir de criterios de partida muy concretos (Janosch, Pérez-Fernández, Nut y Marset, 2023). Por lo demás, y no es menos importante, la información que ofrece el CENDOJ es anónima, pública y se encuentra libre de derechos.

Teniendo en cuenta lo precedente, para la realización del presente estudio se analizaron 76 casos de agresión sexual cometidas por autor inicialmente desconocido por la víctima, en las provincias de Madrid y Barcelona, a partir del análisis de sentencias judiciales publicadas en la base de datos del CENDOJ. El tamaño muestral se corresponde a una representación del total de agresiones sexuales conocidas y juzgadas cometidas por desconocidos en las provincias indicadas. Los criterios de inclusión delineados fueron los siguientes:

1. El asaltante sexual era un varón desconocido para la víctima hasta, al menos, las 24 horas previas al delito, y actuaba siempre en solitario.
2. La víctima, siempre mujer, tenía 16 años o más en el momento de la comisión del delito.
3. Los casos están definidos jurídicamente, en la propia sentencia, como “asaltos sexuales” (penetración efectiva o al menos intentada con pene, por vagina, por boca y/o por ano; o bien penetración efectiva con dedos u otros objetos, por vagina y/o ano).

En función de tales criterios de inclusión se encontraron, casualmente, 38 delitos en la provincia de Madrid y otros tantos en la provincia de Barcelona. Los análisis posteriores se realizaron mediante el paquete estadístico R versión 4.4.2 (2024), *Pile of Leaves*, Copyright (C) 2024 The R Foundation for Statistical Computing. Librerías utilizadas: *vegan, ggplot2, ggrepel, cluster, factoextra, readxl, mclust* y *clue*.

3.1. CATEGORIZACIÓN DE LAS SENTENCIAS

A fin de elaborar adecuadamente los datos de las sentencias para proceder a su posterior análisis estadístico, se han seguido los criterios y nomenclaturas que se describen a continuación:

- Antecedentes judiciales del acusado. Se codifican en las variables denominadas *Ag_Sex* (antecedentes judiciales por delito sexual), *Ag_Theft* (antecedentes judiciales por robo), *Ag_Viol* (antecedentes judiciales por violencia no sexual), y

Ag_Unesp (antecedentes judiciales por delito no especificado). Estas variables se codificaron en la base de datos de la siguiente manera: 0 si el delincuente no tiene antecedentes o problemas psiquiátricos, 1 si los tiene, y 2 si ninguno de estos extremos consta en la sentencia.

- Variables situacionales específicas. Un grupo de siete variables responde a circunstancias situacionales relacionadas con la violación en sí –podrían considerarse como "escenográficas"-. La víctima podría haber ofrecido resistencia a la comisión del delito, o no (*Ver_Resist*); podría haber gritado solicitando ayuda, o no (*Ver_Shout*); podían haberse presentado, o no, durante la comisión del asalto sexual, terceras personas, tales como posibles testigos o fuerzas policiales alertadas por el evento (*Ver_Third*); o bien la violación podría haberse visto interrumpida por alguna causa, o no (*Ver_Inte*). Por lo que respecta al agresor sexual, se asume que éste podría haber actuado bajo el influjo del alcohol (*Ver_Alc*), o de las drogas (*Ver_Drug*), o incluso podría haber tenido sus capacidades volitivas e intelectuales disminuidas (*Ver_Vic*). En todos los casos detectados las variables se codificaron como 0 (ausencia de la conducta), 1 (presencia de la conducta), o 2 (conducta que no consta en la sentencia).
- Conductas sexuales del delincuente. Las siguientes variables asumen tres posibles valores, indicando 0 como ausencia de conducta, 1 como presencia de conducta, y 2 como conducta que no consta en el expediente judicial. Las variables *Ver_Vag*, *Ver_Anal*, y *Ver_Fel* indican que la víctima sufrió penetración con el pene en vagina, ano o boca, respectivamente. Las variables *Ver_Vag_Attempt y Ver_Anal_Attempt* indican que el asaltante sexual intentó sin éxito penetrar con su pene a la víctima por vagina o ano, respectivamente. La variable *Ver_Finger* indica que el agresor penetró a la víctima con los dedos en vagina o ano.
- Conductas no sexuales del agresor. Estas variables también han tomado los valores 0 (ausencia), 1 (presencia), y 2 (no consta). Si el delincuente se acercó a la víctima mediante alguna maniobra de engaño, se codificó la variable *Ver_Con* con 1. Si la atacó de manera sorpresiva, entonces se codificó la variable *Ver_Surp* con 1. Si utilizó algún tipo de arma generalmente un arma blanca) se codificó la variable *Ver_Weap* con 1. Si utilizó algún tipo de vehículo para desplazarse (coche, moto, bicicleta, etcétera) la variable *Ver_Vehi* tomó el valor 1. Si le robó a la víctima algún tipo de valores (dinero, móvil, tarjeta de crédito, etcétera), se codificó la variable *Ver_Val* con 1. Si el robo fue de objetos personales (ropa interior, fotos, agenda, etcétera) que pudieran emplearse con alguna finalidad fetichista, se codificó la variable *Ver_Pers* con 1.
- Otras variables. Surgieron con relación a otras cuestiones alternativas que arrojan las sentencias y que tienen interés para el análisis pormenorizado de los casos. Así:

    a. ¿Mostró el agresor sexual conocimientos forenses en sus conductas (uso de preservativo, guantes, conductas de limpieza y etcétera)? En caso afirmativo se codificó la variable *Ver_Fore* con 1.
    b. ¿Actuó el agresor sexual entre las 22:00 y las 6:00, hora local? Si se dio tal circunstancia la variable *Ver_Darkness* (oscuridad) se codificó como 1.
    c. ¿Actuó el agresor sexual entre el mediodía de un viernes y el mediodía del siguiente lunes? En el caso de que la respuesta a esa cuestión fuese afirmativa la variable *Ver_Wend* (fin de semana) se codificó como 1.

4. RESULTADOS

La Tabla 1 muestra el porcentaje de presencia de las variables anteriormente descritas en las sentencias por agresión sexual referidas a las provincias de Madrid y Barcelona. Como puede observarse en la Tabla 2, dos variables tienen una diferencia significativa entre Madrid y Barcelona, y una variable no es significativa, pero está en el límite de la significación -p≤0,05-. Puede verse, además, que los agresores sexuales actúan más bajo el efecto de las drogas y utilizan más armas en la provincia de Barcelona que en la de Madrid. Sin embargo, se cometen más penetraciones vaginales en los casos detectados Madrid que en los sentenciados en Barcelona.

Tabla 1. Porcentajes de "presencia" de los diferentes comportamientos referidos a los delitos analizados.

Variables	Significado	Madrid	Barcelona
Ag_Sex	Antecedentes judiciales del agresor por delitos sexuales.	5,3%	13,2%
Ag_Theft	Antecedentes judiciales del agresor por robo.	13,2%	13,2%
Ag_Viol	Antecedentes judiciales del agresor por violencia no sexual.	10,5%	10,5%
Ag_Unesp	Antecedentes judiciales por delito no especificado.	15,8%	15,8%
Ver_Resist	La víctima se resistió.	52,6%	60,5%
Ver_Shout	La víctima gritó.	23,7%	28,9%
Ver_Third	Aparecieron terceras personas alertadas.	31,6%	18,4%
Ver_Inte	La agresión sexual fue interrumpida por circunstancias inesperadas.	28,9%	34,2%
Ver_Alc	El agresor estaba bajo los efectos del alcohol.	5,3%	21,1%
Ver_Drug	El agresor estaba bajo los efectos de drogas.	5,3%	28,9%
Ver_Vic	El agresor tenía sus capacidades volitivas e intelectuales disminuidas.	7,9%	18,4%
Ver_Vag	La víctima sufrió penetración vaginal.	76,3%	50,0%
Ver_Anal	La víctima sufrió penetración anal.	7,9%	15,8%
Ver_Fel	La víctima sufrió penetración bucal (felación).	34,2%	47,4%
Ver_Vag_Attempt	Hubo intento de penetración vaginal sin éxito.	7,9%	13,2%
Ver_Anal_Attempt	Hubo intento de penetración anal sin éxito.	10,5%	10,5%
Ver_Finger	El agresor penetró a la víctima con los dedos en vagina o ano.	13,2%	13,2%
Ver_Con	El agresor se acercó a la víctima valiéndose de algún engaño.	55,3%	36,8%
Ver_Surp	El agresor se acercó a la víctima sorpresivamente.	44,7%	63,2%
Ver_Weap	El agresor se valió de algún tipo de arma.	23,7%	47,4%
Ver_Vehi	El agresor se desplazó al lugar de la agresión con algún vehículo.	10,5%	5,3%
Ver_Val	El agresor robó bienes económicos a la víctima.	36,8%	36,8%
Ver_Pers	El agresor sustrajo algún objeto que pudiera emplearse como fetiche.	7,9%	5,3%
Ver_Fore	El agresor demostró tener conocimientos forenses.	5,3%	15,8%
Ver_Darkness	El asalto se cometió entre las 22:00 horas y las 6:00 horas.	42,1%	39,5%

Ver_Wend	El asalto se cometió en fin de semana (entre el mediodía del viernes y el mediodía del lunes).	71,1%	60,5%

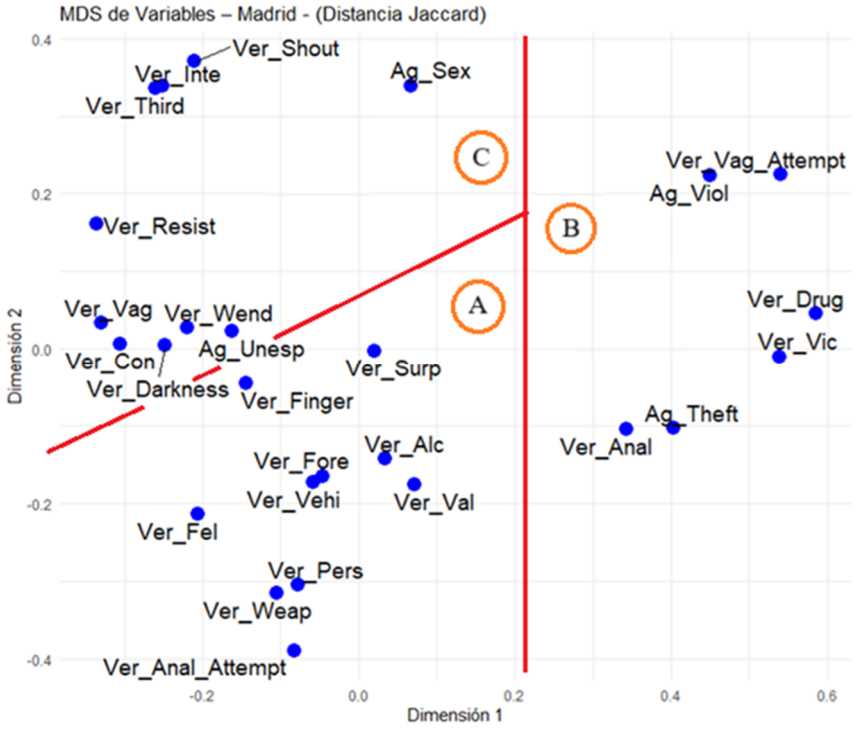
Tabla 2. Variables que han mostrado diferencias significativas entre las agresiones sexuales cometidas por desconocidos en Madrid y Barcelona.

Variable	Valor p	Prueba empleada
Ver_Drug	0,012	Exacta de Fisher
Ver_Vag	0,032	Chi-Cuadrado
Ver_Weap	0,055	Chi-Cuadrado

El resultado del procedimiento de escalamiento multidimensional (MDS) para los casos de Madrid puede observarse en la Figura 1. Los 3 clústeres encontrados (A, B y C, en la figura), conformados por las agrupaciones de los datos y que determinan otras tantas tipologías, se hallaron mediante el análisis de *clustering K-Means*. Las tipologías detectadas en la provincia de Madrid, analizadas independientemente, quedarían como sigue:

- El tipo A, de corte impulsivo, es una persona con antecedentes por otras agresiones sexuales que suele actuar en la oscuridad, durante el fin de semana, y que se aproxima a la víctima valiéndose de alguna clase de subterfugio. Sin embargo, muchas veces la víctima se resiste y grita alertando a terceros, con lo que la violación, pese a la existencia de penetración anal o vaginal, se ve interrumpida. No obstante, podrá robar a la víctima objetos de valor.
- El tipo B, de naturaleza versátil, nos muestra a un agresor sexual que opera bajo la influencia de las drogas y que, por lo tanto, tiene sus capacidades intelectuales y/o volitivas disminuidas. En este caso, en el que el agresor podría tener antecedentes por robo y otros delitos violentos, suele existir intento de penetración vaginal, pero sin éxito, así como penetración anal. Posiblemente, cabría pensar en una persona con el raciocinio alterado, inicialmente motivada por el robo, que trata de aprovechar la ocasión.
- El tipo C sugiere la presencia de un agresor sexual planificador y más especializado, con alguna conciencia forense, que se desplaza en un vehículo y que se sirve durante la agresión de alguna clase de arma para intimidar y someter la voluntad de sus víctimas. En este caso suele existir consumo de alcohol por parte del agresor, que obligará al a víctima a practicarle una felación, podrá intentar la introducción vaginal mediante los dedos y tratará de realizar una penetración anal. Este tercer tipo de agresor suele llevarse objetos de la víctima que utilizará como fetiches o trofeos.

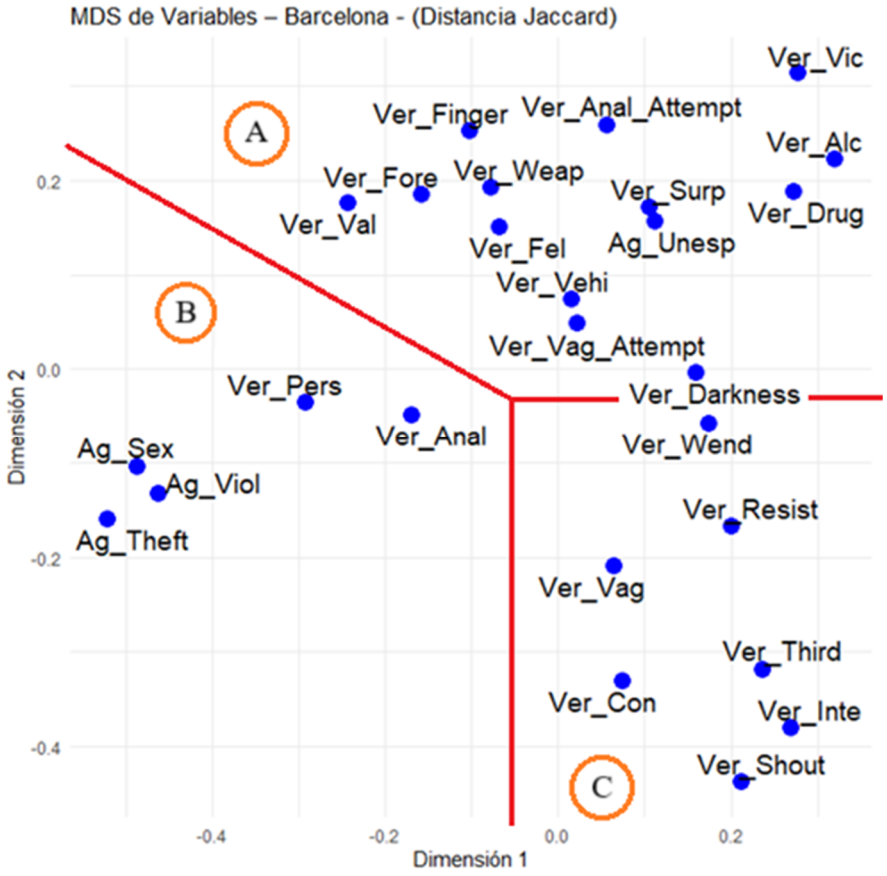
Figura 1. Escalamiento multidimensional de las agresiones sexuales cometidas en Madrid.



El resultado del MDS para los casos de la provincia de Barcelona puede verse en la Figura 2. Al igual que en el caso precedente, los 3 clústeres (A, B y C en la figura), conformados por las agrupaciones de los datos, se hallaron mediante el análisis de *clustering K-Means*. Las tipologías detectadas en la provincia de Barcelona quedarían como sigue:

- El tipo A, de sesgo ocasional, sería una persona con cierta conciencia forense, que se desplaza en un vehículo, consume drogas y tiene antecedentes por otros delitos no especificados en la sentencia. Esta persona, que suele actuar empleando armas para someter a la víctima y bajo los efectos de drogas y alcohol, se acerca a sus víctimas sorpresivamente y puede tratar de forzarlas a realizarle una felación. Intentará, tras introducir los dedos en los genitales de la víctima, e indistintamente, de proceder a la penetración anal y/o vaginal, pero no suele tener éxito.
- El tipo B, muy versátil, polidelincuente y por lo tanto poco definido, es un agresor con antecedentes por otros delitos sexuales, por robo y por violencia no sexual, que sustraerá de la víctima objetos sin valor aparente que pueda emplear como fetiches.
- El tipo C, de sesgo ocasional y recreativo, opera durante la noche y generalmente en fines de semana. Se acerca a la víctima mediante engaños y/o subterfugios varios a fin de proceder a la penetración vaginal, pero al no haber armas o planificación previa que facilite sus actividades, la víctima se resistirá, gritará y alertará a terceros que posiblemente interrumpirán el asalto.

Figura 2. Escalamiento multidimensional de las agresiones sexuales cometidas en Barcelona.

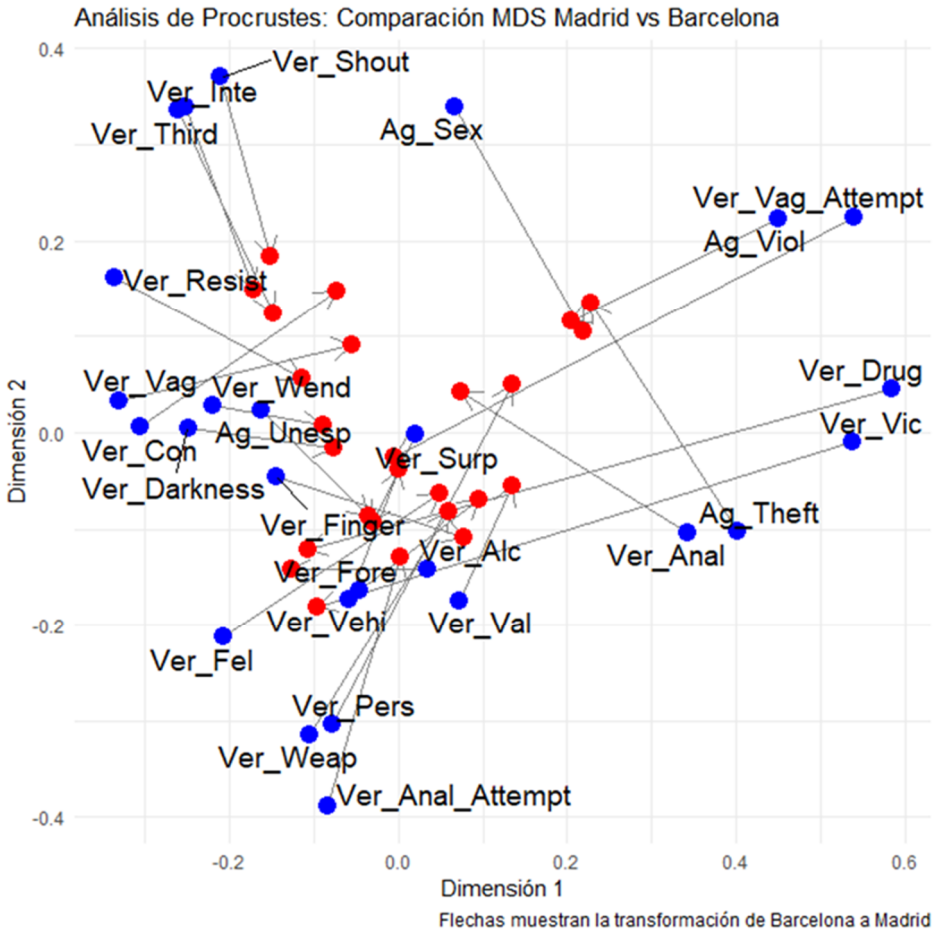


Con la finalidad de proceder a una comparativa entre las agresiones y tipologías presentes en ambos contextos, se ha aplicado la prueba de Procrustes a los escalamientos multidimensionales (MDS) que muestran los clústeres/tipologías de Madrid y Barcelona, de manera tal que se logre el mejor ajuste entre ambos. Realizado este proceso, se han calculado el Índice de Jaccard (0,393) y el Índice ARI (0,332). Ello ha dado como resultado una superposición y diferenciación de las tipologías descritas para cada uno de los entornos delincuenciales. La Figura 3 aparece como resultado de la prueba de Procrustes destinada a comparar el resultado del MDS aplicado a los datos de Madrid con el resultado del MDS aplicado a los datos de Barcelona[4]. Se significa en este punto que el análisis de Procrustes es útil para evaluar la similitud entre dos configuraciones -o nubes- espaciales de datos. Los resultados obtenidos mediante este procedimiento, por lo tanto, muestran cómo se alinean las configuraciones espaciales de los datos de Madrid y

[4] El análisis de Procrustes es un proceso de transformación euclidiana inserto en la serie de métodos estadísticos que aplican la teoría de grupos al análisis de conjuntos de datos homogéneos, a fin de poder compararlos entre sí y realizar inferencias desde dichas comparaciones. Forma parte de los procedimientos insertos en el llamado "análisis estadístico multivariable". Su nombre procede del mito de Procusto, uno de los hijos de Poseidón que, además, resultó ser un terrible asesino serial. Este tenía una casa donde ofrecía alojamiento a los viajeros cansados que se aventuraban por aquellos pagos. Allí los invitaba a tumbarse en una cama de hierro a la que, entretanto dormían, ataba de pies y manos a sus cuatro esquinas. Si la víctima propiciatoria era tan alta que su cuerpo resultaba más largo que la cama, Procusto procedía a aserrar las partes del cuerpo que sobresalían. Si era de menor longitud que el lecho, entonces descoyuntaba a la víctima a martillazos para estirarla hasta las dimensiones adecuadas. (Hurley y Cattell, 1962; Gower, 1975).

Barcelona tras una transformación óptima (rotación, escalado y traslación) destinada a minimizar lo más posible las diferencias entre ambas.

Figura 3. Comparación entre los EMD de las provincias de Madrid y Barcelona.



4.1. TIPOLOGÍAS A

En el caso de Madrid, como se ha indicado anteriormente, este clúster agrupa variables relacionadas con delitos donde hay un robo de objetos o una agresión menos violenta en términos físicos. En Barcelona, sin embargo, dentro de este clúster predominan agresores con antecedentes por delitos violentos y robos, sin variables que indiquen directamente violencia sexual consumada.

Las principales diferencias entre ambos entornos tienen que ver con los antecedentes criminales, pues en el caso de Barcelona hay una elevada presencia de agresores con antecedentes por delitos sexuales, robo y violencia. En Madrid, sin embargo, el clúster está más relacionado con el robo de bienes materiales, trofeos o fetiches. También en lo tocante a la agresión sexual propiamente dicha se pueden encontrar variaciones significativas. Mientras que en los casos de la provincia de Barcelona hay una mayor relación con penetración anal, en Madrid se observan intentos de penetración anal sin éxito y agresiones con los dedos o felaciones.

Como regla general, podría indicarse que en el clúster A, para Madrid, hay más casos de engaño, subterfugio o excusa para acercarse a la víctima y robo, mientras que en Barcelona el historial criminal del agresor se convierte en un factor clave que se ha de tener en cuenta a la hora de evaluar su peligrosidad potencial.

4.2. TIPOLOGÍAS B

En lo tocante a Madrid, las variables incluidas en este clúster indican un perfil de agresores con antecedentes judiciales por delitos violentos y/o sexuales, así como circunstancias en las que el agresor está bajo los efectos de diversas sustancias. La víctima, por su parte, sufre agresiones sexuales consumadas o intentos de estas. Con respecto a Barcelona las variables aportan un perfil de agresores sin antecedentes penales específicos, pero con características que reflejan una clara planeación del ataque y un consumo de sustancias.

Las diferencias principales en lo que respecta a los antecedentes criminales ofrecen, para Madrid, una presencia más clara de antecedentes por robo y violencia, entretanto que en Barcelona hay una categoría bastante más ambigua de antecedentes no especificados. Sobre el modo de operar del agresor, en los casos de Barcelona hay mayor indicio de planeación, como pone de manifiesto la presencia muy sistemática de uso de engaños, vehículos y armas. En Madrid, sin embargo, la violencia directa parece jugar un papel mucho más relevante.

Con respecto al uso de sustancias y a la agresión sexual en sí misma, en ambos casos se observa la presencia de drogas o alcohol, pero en Madrid la violencia sexual es más evidente en términos de agresiones consumadas. En Barcelona, dentro del tipo B, hay una mayor tendencia a los intentos de agresión sin éxito, pero con métodos más diversos como la penetración con los dedos.

4.3. TIPOLOGÍAS C

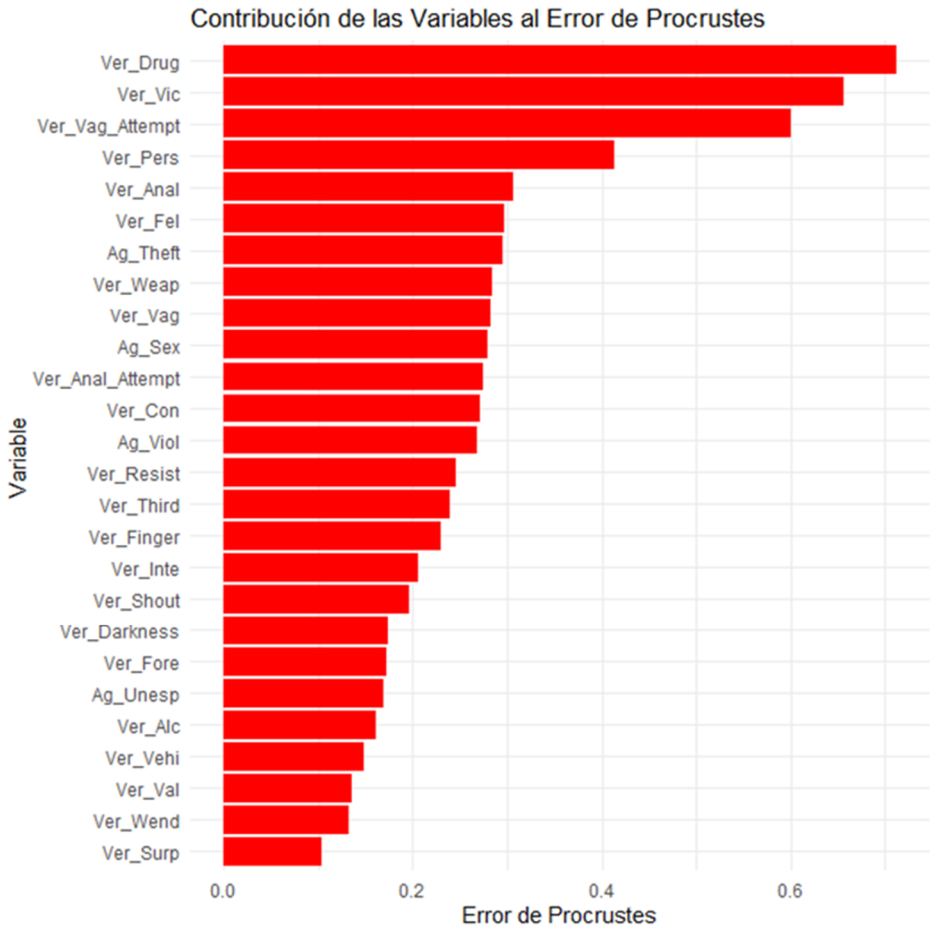
En el contexto de Madrid las variables en este clúster reflejan a agresores que no necesariamente tienen antecedentes judiciales graves, pero que operan impulsivamente, sin mucha planificación y en entornos donde la víctima intenta resistirse y suele producirse una intervención de terceros. En el caso de Barcelona se encuentran también ataques interrumpidos, pero con menos énfasis en el uso de engaños para aproximarse a la víctima y con una menor intervención de terceros que puedan frustrar el ataque.

Las principales diferencias, en lo que respecta a los antecedentes criminales, tienen que ver en Madrid, con el hecho de que este grupo incluye agresores con antecedentes por delitos sexuales, mientras que en Barcelona no se mencionan tales antecedentes criminales. Como se decía, además, en ambos casos hay resistencia de la víctima y una posible interrupción del ataque, pero en Madrid hay más variables asociadas a la presencia de terceros. Del mismo modo, en las agresiones de la provincia de Madrid la ocurrencia nocturna es un factor más fuerte, entretanto que en Barcelona la variable de nocturnidad no aparece dentro de este clúster.

La Figura 4, por otra parte, resulta ilustrativa en la medida que representa la contribución de cada variable al error de Procrustes -es decir, al desajuste de ambos conjuntos de datos-. Ello indica qué aspectos de la agresión difieren más entre las

configuraciones de datos halladas entre los clústeres de Madrid y Barcelona tras la transformación.

Figura 4. Diferencias de cada una de las variables en la posición espacial de los MDS obtenidos con los datos de Madrid y los datos de Barcelona.



Cuando se atienden a la interpretación general de los resultados descritos, se han de tener en cuenta, por otro lado, diversos elementos:

1. Número de objetos y dimensiones: se compararon 26 variables en un espacio de 2 dimensiones.
2. Medida del ajuste (suma de cuadrados de Procrustes): 2,6286, indica el nivel de diferencia entre las configuraciones antes y después de la transformación.
3. Error cuadrático medio de Procrustes (RMSE): 0,31796, representa la magnitud promedio del error en la alineación de los puntos (Tabla 3).

Tabla 3. Distribución de los errores cuadráticos medios encontrados en el análisis Procrustes.

Mínimo error	0,1041
Primer cuartil (Q1)	0,1719
Mediana	0,2568
Tercer cuartil (Q3)	0,2919
Máximo error	0,7121

Teniendo en cuenta todo lo indicado, lo que los datos de la Tabla 3 sugieren, pues, es que la mayoría de las variables tiene un error de ajuste relativamente bajo, pero hay algunas con errores más elevados. En todo caso, para lograr el mejor ajuste posible de los gráficos presentados en las figuras 1 y 2, se debió hacer una rotación de 180º, con una traslación prácticamente nula, y un escalado de aproximadamente 0,5. Esto no implicó una alteración significativa de los resultados y respondió al hecho de que el gráfico de la provincia de Barcelona tenía un tamaño lineal de aproximadamente la mitad del obtenido con los datos de la provincia de Madrid, lo cual impedía establecer las adecuadas comparaciones. El hecho es que las configuraciones de Madrid y Barcelona son similares en estructura, pero arrojan diferencias en lo referente a la escala y orientación. Esto, por sí mismo, ya indica que existen diferencias entre los datos de ambas provincias que no pueden soslayarse y que, por lo tanto, se está ante realidades diferentes con relación a la materia estudiada. Así, aunque la correspondencia entre los conjuntos de datos es aceptable, algunos puntos presentan errores más altos que indican diferencias en la manera en que se estructuran ciertos tipos de agresión -y de comportamientos del agresor- en ambas provincias.

Hecha esta aclaración, si ahora se realiza una observación más detenida de la Figura 3, se advierte que los puntos azules representan la configuración original de Madrid antes de la transformación, mientras que los puntos rojos representan la configuración transformada de Barcelona a fin de alinearse con la de Madrid. Las flechas muestran la magnitud y sentido del ajuste necesario para alinear Barcelona con Madrid. Como se vio en los resultados numéricos, la estructura de Barcelona fue rotada casi 180°, además de escalada a partir del procedimiento de Procrustes, para alinearla con Madrid. Esto se hace patente porque algunos puntos azules y rojos están en posiciones opuestas en ciertas zonas. Los puntos con líneas más largas relacionando la misma variable indican que hubo diferencias significativas en la representación de esa variable entre ambas ciudades. Por ejemplo, *Ver_Drug*, *Ver_Vic* y *Ver_Vag_Attempt* muestran desplazamientos grandes, sugiriendo que en Madrid su representación espacial en el MDS es distinta a la de Barcelona.

Por otro lado, en las áreas con mayor concordancia, es decir, donde las variables en las que los puntos rojos y azules están cerca, se sugieren estructuras similares en ambas provincias. Por ejemplo: *Ver_Finger*, *Ver_Fore* y *Ver_Alc* muestran un menor desplazamiento, lo que indica que sus patrones son similares en ambas ciudades. La estructura general de los tipos de agresiones y de comportamientos adheridos a ellas es similar en ambas ciudades, pero con interesantes diferencias en orientación y escala. Como ya vimos, algunas variables muestran mayor discrepancia, como en los casos de *Ver_Drug*, *Ver_Vic* y *Ver_Vag_Attempt*, lo que indica que estos factores se perciben o estructuran de manera distinta en cada provincia. Otras variables tienen estructuras similares, lo que sugiere patrones comunes de agresión y respuesta en ambas ciudades que la criminología debería explicar en aras a profundizar en su campo de investigación y no simplemente asumir.

Tales diferencias en las estructuras de los correspondientes MDS de Madrid y Barcelona hay que relacionarlas, necesariamente, con las tipologías halladas mediante el procedimiento de *K-Means*. Retórnese ahora a la Figura 4, pues ayudará a clarificar numéricamente lo que sucede. Las variables con mayor error de Procrustes -es decir, las que más difieren entre ambas ciudades- son:

- *Ver_Drug* (0,71): El agresor estaba bajo los efectos de drogas.
- *Ver_Vic* (0,66): El agresor tenía sus capacidades volitivas e intelectuales disminuidas.
- *Ver_Vag_Attempt* (0,60): Hubo intento de penetración vaginal sin éxito.
- *Ver_Pers* (0,41): El agresor sustrajo algún objeto que pudiera emplearse como fetiche.
- *Ver_Anal* (0,30): La víctima sufrió penetración anal.
- *Ver_Fel* (0,29): La víctima sufrió penetración bucal (felación).
- *Ag_Theft* (0,29): Antecedentes judiciales del agresor por robo.
- *Ver_Weap* (0,28): El agresor se valió de algún tipo de arma. Hay diferencias en las agresiones en las que el agresor usa un arma, siendo de mayor frecuencia en Barcelona.
- *Ver_Vag* (0,28): La víctima sufrió penetración vaginal.

5. DISCUSIÓN

Parece evidente que el estudio comparativo entre las agresiones sexuales cometidas por desconocidos en las provincias de Madrid y de Barcelona ha revelado diferencias significativas en la forma en que se perpetran estos delitos en cada uno de los contextos y que, por lo tanto, la hipótesis de partida se cumple. A partir del análisis de 76 casos extraídos de sentencias judiciales y examinados mediante pruebas estadísticas robustas -prueba exacta de Fisher, chi-cuadrado, escalamiento multidimensional y análisis de Procrustes-, se han identificado patrones distintivos en las agresiones sexuales cometidas en ambos territorios.

En cuanto a la pertinencia de los estadísticos utilizados, el uso de la prueba exacta de Fisher y chi-cuadrado para comparar la presencia de ciertas características en los delitos cometidos en Madrid y Barcelona permitió establecer diferencias significativas -o casi significativas- en aspectos clave como el consumo de drogas por parte del agresor (*Ver_Drug*, $p = 0{,}012$), el uso de armas (*Ver_Weap*, $p = 0{,}055$, en el límite de significación), y la penetración vaginal (*Ver_Vag*, $p = 0{,}032$). Estas pruebas fueron apropiadas para evaluar asociaciones entre variables categóricas en un conjunto de datos representativo, pero relativamente pequeño.

El MDS y el análisis *K-means* permitieron identificar tipologías de agresores y patrones de agresión en cada provincia, mostrando diferencias estructurales en la manera en que estos delitos son cometidos. El análisis de Procrustes demostró -siempre dentro de la muestra de referencia, lo cual ha de inducir a una razonable cautela- que, aunque existe una estructura similar en las agresiones sexuales de ambas áreas, la escala y orientación de los factores difieren significativamente, indicando patrones específicos en cada una de ellas.

En cuanto a las diferencias entre Madrid y Barcelona el análisis estadístico y espacial de los datos ha revelado que, si bien los delitos sexuales cometidos por desconocidos presentan similitudes estructurales en Madrid y Barcelona, hay diferencias importantes en los métodos y circunstancias de las agresiones que apelan a la importancia de un estudio detallado de ambos ecosistemas delincuenciales, tal y como se comentó en la introducción, y como pronostica la TAS:

- Mayor consumo de drogas por parte de los agresores en Barcelona: Un 28,9% de los agresores estaban bajo los efectos de drogas en el momento del delito, en comparación con solo el 5,3% en Madrid. Esto podría indicar una mayor asociación entre consumo de sustancias y agresividad en Barcelona o un contexto criminológico diferente en el que los agresores de esa ciudad tienen un mayor historial de consumo de drogas en el momento del ataque.
- Mayor uso de armas en la provincia de Barcelona: un 47,4% de los agresores emplearon algún tipo de arma para someter a la víctima, mientras que en Madrid este porcentaje fue del 23,7%. Esto sugiere un mayor grado de violencia instrumental en las agresiones cometidas en Barcelona, lo que podría estar relacionado con factores ambientales o criminológicos específicos del contexto.
- Diferencias en la forma de perpetrar la agresión sexual: en Madrid, la penetración vaginal fue más frecuente (76,3%) en comparación con Barcelona (50%). Pero, por otro lado, las agresiones con penetración bucal (felación) fueron más frecuentes en Barcelona (47,4%) que en Madrid (34,2%). De igual forma, la penetración anal también fue más común en Barcelona (15,8%) que en Madrid (7,9%).
- Diferencias en la estrategia de aproximación del agresor: en Madrid, los agresores emplearon más estrategias de engaño, distracción o subterfugio para acercarse a la víctima (55,3%) que en Barcelona (36,8%). En contraste, en Barcelona se observó una mayor cantidad de ataques sorpresivos y no planificados (63,2% frente a 44,7% en Madrid). Esto sugiere que los agresores de la provincia de Barcelona optan con mayor frecuencia por ataques directos y violentos, entretanto que los de Madrid apelan más al uso de manipulación y el engaño para reducir la resistencia de la víctima potencial.
- Diferencias en la respuesta de la víctima y la interrupción del delito: las víctimas, en Barcelona, tendieron a resistirse en mayor proporción (60,5%) en comparación con Madrid (52,6%). Quizás por ello la interrupción de la agresión por circunstancias inesperadas fue más frecuente en Barcelona (34,2%) que en Madrid (28,9%), lo que sugiere que en Barcelona las agresiones tenderían a producirse en contextos menos controlados por el agresor, hecho que tiene sentido puesto en consonancia con la idea del mayor uso de la violencia, y, por tanto, de un componente de mayor impulsividad y un menor control práctico de la escena en el agresor sexual desconocido de la provincia de Barcelona.
- Antecedentes penales del agresor: los agresores, en Barcelona, presentaron mayor número de antecedentes por delitos sexuales previos (13,2%) en comparación con Madrid (5,3%). No hubo, sin embargo, diferencias significativas en los antecedentes por robo o violencia no sexual.

6. CONCLUSIONES

A partir de los hallazgos descritos en el presente estudio, es posible describir un perfil de las agresiones sexuales por desconocidos halladas en las sentencias emitidas en cada una de las provincias analizadas.

En Madrid existió un mayor uso del engaño para acercarse a la víctima, una mayor frecuencia de penetración vaginal, un menor uso de armas y drogas en el momento de la agresión, y un colectivo de agresores con menos antecedentes por delitos sexuales previos. En Barcelona, por otro lado, existió una mayor frecuencia de ataques sorpresa, un mayor uso de armas y drogas, y un mayor número de agresores con antecedentes

penales por delitos sexuales. También se detectó una mayor frecuencia de agresiones con penetración bucal y anal, y una mayor tendencia de la víctima a resistirse, aunque con una mayor proporción de agresiones interrumpidas por factores externos.

Los resultados de este estudio confirman que las agresiones sexuales perpetradas por desconocidos presentan diferencias significativas en ambos territorios, lo que sugiere la necesidad de estrategias de prevención y respuesta adaptadas a las características criminológicas específicas de cada ciudad. Esto, en el contexto de la TAS, sólo sería posible prestando atención a una análisis pormenorizado del contexto delincuencial-criminal en el que los agresores actúan en cada caso, por lo que requeriría de estudios concretos, específicos, detallados y pormenorizados que, sencillamente, ponen en tela de juicio la validez de las grandes teorías y metodologías -que explican con ciertas garantías lo general, pero suelen fracasar en su acercamiento a lo particular- e imponen la necesidad un estudio quirúrgico de cada ecosistema criminal a fin de concretar políticas -de detección, de investigación, de prevención- precisas y eficientes. Así, por ejemplo, este trabajo sugiere que en la provincia de Barcelona, dado el mayor uso de armas y drogas en los ataques, convendría implementar las pertinentes medidas de control sobre estos aspectos, a la par que proceder a un estudio más profuso, detallado y atinado del historial criminal de los agresores potenciales. En Madrid, sin embargo, la marcada tendencia detectada al empleo del del engaño en la aproximación a la víctima potencial por parte del agresor sexual podría indicar la necesidad de campañas de concienciación que ayuden a las mujeres a identificar en los desconocidos el empleo de posibles estrategias de manipulación, control y aislamiento.

Desde una perspectiva criminológica, y siempre atendiendo a las variables ecosistémicas, los hallazgos destacan la importancia de seguir investigando la relación entre los antecedentes penales -su carrera delictiva previa, en general- de los agresores y su conducta durante la agresión, así como las diferencias detectables en la respuesta concreta de las víctimas y de los factores que pueden llevar a la interrupción de un ataque, lo cual puede sugerir avances y desarrollos interesantes en el marco de las políticas criminales a nivel autonómico e incluso provincial.

Debe hacerse notar, por otro lado, la relevancia de este estudio para el desarrollo de técnicas criminalísticas auxiliares a la investigación policial, y más concretamente al crecimiento de la perfilación -análisis de conducta- criminológica inductiva, pues los datos encontrados sirven a la matización detallada de tipologías criminales vigentes que a menudo, por excesivamente amplias, tienden a ser poco útiles en lo que refiere a su aplicación práctica. Vemos, por ejemplo, que la provincia de Madrid los agresores tienen clústeres más diferenciados en función de la gravedad del delito que se comete, mientras que en la provincia de Barcelona el agresor muestra una organización conductual más vinculada a su historial criminal concreta. En ambos casos, indistintamente, el consumo de sustancias y la planificación del ataque juegan un papel relevante, pero existen claras diferencias en lo tocante a la ejecución y la interrupción del crimen que debieran conocerse y matizarse adecuadamente, pues ayudarían mucho en lo referente al diseño de perfiles criminales específicos, así como a los procesos de investigación policial.

En definitiva, este estudio, que aquí solo aborda dos provincias, pero podría ampliarse a nivel nacional con la adecuada financiación e infraestructura, contribuye a una mejor comprensión de la violencia sexual por desconocidos, a la par que muestra que un estudio situacional-ecológico del crimen no sólo proporciona datos útiles para mejorar

la prevención, intervención y persecución del delito, sino también su comprensión criminológica misma más allá de generalidades.

7. REFERENCIAS BIBLIOGRÁFICAS

Arqué-Valle, P., Pastor-Cárcel, A., Roca-Mercadé, C. y Soria M.A. (2024). Influencia cultural en la motivación sexual de los asesinos seriales. *Revista Logos Ciencia & Tecnología, 16*(1), 145-159, doi: https://doi.org/10.22335/rlct.v16i1.1908

CGPJ (2023). Los tribunales han acordado 1.205 reducciones de pena en aplicación de la Ley Orgánica 10/2022 [disponible en: **https://www.poderjudicial.es/cgpj/es/Poder-Judicial/Consejo-General-del-Poder-Judicial/En-Portada/Los-tribunales-han-acordado-1-205-reducciones-de-pena-en-aplicacion-de-la-Ley-Organica-10-2022**, recogido marzo de 2024].

Corovic, J., Christianson, S.A. y Bergman, R. (2012). From crime scene actions in stranger rape to prediction of rapist type: single victim or serial rapist? Behavioral Science and the Law, 30, 764-781.

Domínguez Vela, M. (2016). Violencia de género y victimización secundaria. Revista Digital de Medicina Psicosomática y Psicoterapia, Vol. 6(1). [disponible en: **https://www.psicociencias.org/pdf_noticias/Violencia_de_geneo_y_victimizacion_secundaria.pdf**, recogido en mayo 2024].

Gower, J.C. (1975). Generalized Procrustes analysis. Psychometrika, 40, 33–51.

Gutiérrez de Piñeres Botero, C., Coronel, E. y Pérez, C.A. (2009). Revisión teórica del concepto de victimización secundaria. Liberabit [online], 15(1), 49-58 [disponible en: **https://pepsic.bvsalud.org/scielo.php?script=sci_abstract&pid=S1729-48272009000100006**, recogido marzo 2024].

Hurley, J. R., y Cattell, R. B. (1962). The Procrustes Program: Producing direct rotation to test a hypothesized factor structure. Behavioral Science, 7(2), 258-262. **https://doi.org/10.1002/bs.3830070216**

Janosch González, H. (2013). Fundamentos filosóficos de la criminología en Hirschi y Wikström. ¿Popper o Bunge? En Serrano Maíllo, A., y Birkbeck, C., (Eds.) La Generalidad de la Teoría del Autocontrol. Una primera extensión de la teoría general del delito a los países de habla hispana. Madrid: Editorial Dykinson.

Janosch, H., Pérez-Fernández, F., Nut, D. y Marset, M. (2023). Asaltantes sexuales desconocidos para la víctima en España. Un análisis mediante escalamiento multidimensional (EMD) a partir de un análisis de sentencias. Revista de Derecho Penal y Criminología, 3ª Época, 30, 395-411.

Janosch, H., Pérez-Fernández, F. y Herrero, S. (2025). Asaltantes sexuales desconocidos para la víctima en la Comunidad de Madrid: un análisis exploratorio a partir de sentencias condenatorias de la Audiencia Provincial. H. Janosch y F. Pérez-Fernández (coords.), Panorámica de los delitos sexuales en España. Madrid: Dykinson, 43-85.

Janosch, H., Pérez-Fernández, F. y Popiuc, M. (2023). Bajo autocontrol en hombres no-heterosexuales como predictor de comportamientos de agresión sexual contra mujeres. Behavior & Law Journal, 9(1), 65-79, **https://doi.org/10.47442/blj.2023.100**

Janosch, H., Pérez-Fernández, F., Popiuc, M. y López-Muñoz F. (2024). Relationship between low personal morality and impersonal sex with sexual aggression behaviors towards women in a sample of Spanish heterosexual men. Journal of Asia Pacific Studies, 7(2), 109-139.

Janosch González, H., Pérez-Fernández, F. y Soto Castro, J.E. (2020). Un modelo de perfilación para agresores sexuales desconocidos que agreden en las entradas de los edificios. Revista de Derecho Penal y Criminología, 3ª época, 24, 243-258.

Kühne, H.H. (1986). Kriminologie: Victimologie der Notzucht. Juristische Schulung, 5, 388-394.

Linde, A. y Aebi, M.F. (2021). ¿Realmente theft quiere decir hurto? y otras equivalencias dudosas entre las definiciones legales y criminológicas de las infracciones. Consecuencias para el estudio de la delincuencia. Revista Española de Investigación Criminológica, 19, Extra-2 [www.criminologia.net], **https://doi.org/10.46381/reic.v19i2.529**.

Ministerio del Interior de España (2023). Anuario Estadístico del Ministerio del Interior 2022. Catálogo de Publicaciones de la Administración General del Estado: **https://cpage.mpr.gob.es**

Pauwels, L., 2018a. Analysing the perception-choice process in Situational Action Theory. A randomized scenario study. European Journal of Criminology, 19(1), 130-147.

Pauwels, L. (2018b). The conditional effects of self-control in situational action theory. A preliminary test in a randomized scenario study. Deviant Behavior.

Pérez-Fernández, F., Janosch, H. y Popiuc, M. (2023). Bajo autocontrol en hombres no-heterosexuales como predictor de comportamientos de agresión sexual contra mujeres. Behavior & Law Journal, 9(1), 65-79. **https://doi.org/10.47442/blj.2023.100**

Pueyo, A.A. y Redondo Illescas, S. (2007). Predicción de la violencia. Entre la peligrosidad y la valoración del riesgo de violencia. Papeles del Psicólogo, 28(3), 157-173.

Serrano Maíllo, A. (2017). Delito, moralidad individual y controles. Valencia: Tirant Lo Blanch.

Triviño, C., Winberg, M. y Moral, M. (2021). Credibilidad del Testimonio en Agresiones y Abusos Sexuales a Menores: Evolución de los Testimonios no Creíbles en la Última Década. Behavior & Law Journal, 7(1), 43-57. **https://doi.org/10.47442/blj.v7.i1.83**

Wikström, P.-O., Oberwittler, D., Treiber, K. & Hardie, B. (2012). Breaking Rules: The Social and Situational Dynamics of Young People's Urban Crime. Oxford: Oxford University Press.

Wikström, P.-O., & Treiber, K. (2016). Social Disadvantage and Crime: A Criminological Puzzle. American Behavioral Scientist 60(10), 1232–1259.

Revista Científica del Centro Universitario de la Guardia Civil
Revista Logos Guardia Civil

Artículo de Investigación

DROGAS Y CONDUCCIÓN: "TOLERANCIA CERO" METODOLOGÍA DEL INFORME SALIVAL DEL LABORATORIO SYNLAB Y CRITERIOS DE HOMOLOGACIÓN DE LA ENTIDAD NACIONAL DE ACREDITACIÓN

Juan Carlos Rodríguez Bello
Cabo 1º de la Guardia Civil
Agrupación de Tráfico de la Guardia Civil
Experto Universitario en Delincuencia Vial por la UNED
Perito Judicial en Documentoscopia por la UNED
jcrbello@guardiacivil.es

Recibido 18/02/2025
Aceptado 14/05/2025
Publicado 27/06/2025

Cita recomendada: Rodríguez, J. C. (2025). Drogas y conducción: "tolerancia cero" metodología del informe salival del laboratorio Synlab y criterios de homologación de la Entidad Nacional de Acreditación. *Revista Logos Guardia Civil*, 3(2), p.p. 197-220.

Licencia: Este artículo se publica bajo la licencia Creative Commons Atribución-NoComercial-SinDerivadas 4.0 Internacional (CC BY-NC-ND 4.0)
Depósito Legal: M-3619-2023
NIPO en línea: 126-23-019-8
ISSN en línea: 2952-394X

DROGAS Y CONDUCCIÓN: "TOLERANCIA CERO" METODOLOGÍA DEL INFORME SALIVAL DEL LABORATORIO SYNLAB Y CRITERIOS DE HOMOLOGACIÓN DE LA ENTIDAD NACIONAL DE ACREDITACIÓN

Sumario: 1. INTRODUCCIÓN. 2. ESTRATEGIA DE LA DIRECCIÓN GENERAL DE TRÁFICO: "TOLERANCIA CERO". 2.1. FUNDAMENTACIÓN Y PROCEDIMIENTO PARA LA REALIZACIÓN DE LA PRUEBA SALIVAL DE DROGAS. 3. LA DOCTRINA DE LA FISCALÍA GENERAL DEL ESTADO TRAS EL "POSITIVO" SALIVAL INDICIARIO EN DROGAS. 4. PRESENCIA DE DROGAS EN EL ORGANISMO: LA SANCIÓN ADMINISTRATIVA Y LA DOCTRINA DEL TRIBUNAL CONSTITUCIONAL. 5. LOS "PUNTOS DE CORTE" Y LAS CANTIDADES MÍNIMAS PSICOACTIVAS. 6. LA EMPRESA DE ANÁLISIS CLÍNICOS SYNLAB. 7. LÍMITES DE CUANTIFICACIÓN Y RANGOS DE INCERTIDUMBRE DEL LABORATORIO SYNLAB. 8. EL LABORATORIO SYNLAB Y SU HOMOLOGACIÓN POR LA ENTIDAD NACIONAL DE ACREDITACIÓN MEDIANTE AUDITORÍAS. 9. ALCANCE DE LA ACREDITACIÓN ENAC 1169/LE2347 EXPEDIDO A LABORATORIOS SYNLAB. 10. CONCLUSIONES. 11. REFERENCIAS BIBLIOGRÁFICAS. ANEXO I – COMPOSICIÓN Y PRINCIPIOS DEL DED (ANALIZADOR) SOTOXA.

Resumen: La legislación sobre el control del consumo de alcohol y drogas tiene una gran repercusión en la sociedad, no siempre exenta de polémica, dependiendo de cómo se traslade esta información a la opinión pública. Un claro ejemplo, lo tenemos con los criterios que se utilizan para establecer el límite legal de consumo de alcohol compatible con la conducción. Si bien es aceptado por la sociedad el criterio de tolerancia cero en cuanto al consumo de drogas, es fundamental la estandarización de los métodos por los que se detecta y cuantifica la presencia de drogas que influye en la conducción y, consecuentemente, afecta a la Seguridad Vial. En este contexto, establecer y determinar la cantidad de las concentraciones mínimas, en caso de detectarse un positivo en drogas, es imprescindible y especialmente importante en conductores reincidentes o en los delincuentes viales. Sin embargo, esta determinación cualitativa y cuantitativa debe estar debidamente auditada. En este artículo, se hace una revisión del histórico que ha llevado a la determinación de las cantidades detectables de drogas, pero, sobre todo, a los criterios de trazabilidad que son propios de sistemas acreditados en el ámbito de la Seguridad Vial.

Abstract: Legislation on the control of alcohol and drug consumption has a significant impact on society—often not without controversy—depending on how this information is communicated to the public. Clear examples include the criteria used to establish the legal alcohol limit compatible with driving. Although the zero-tolerance criterion for drug consumption is widely accepted by society, it is essential to standardize the methods used to detect and quantify the presence of drugs that impair driving and, consequently, affect road safety. In this context, establishing minimum concentration thresholds in the event of a positive drug test is crucial, particularly in the case of repeat or serious traffic offenders.

However, this qualitative and quantitative determination must be properly audited. This article reviews the historical development that has led to the establishment of detectable drug quantities, with a particular focus on the traceability criteria typical of accredited systems in the field of road safety.

Palabras clave: Seguridad Vial, tolerancia cero, conducción, drogas, detección, concentración mínima, estandarización, acreditación

Keywords: Road safety, zero tolerance, driving, drugs, detection, minimum concentration, standardization, accreditation.

ABREVIATURAS

Art.: Artículo.

CP: Código Penal.

DED: Dispositivo Electrónico de Detección (de drogas portátil).

DGT: Dirección General de Tráfico.

ENAC: Entidad Nacional de Acreditación

FSCSV: Fiscal de Sala Coordinador de Seguridad Vial

FGE: Fiscalía General del Estado.

ISO: International Stantarization Organization (estándar reconocimiento internacional).

LOQ: Limit Of Quantification (límite de cuantificación).

LSV: Ley de Seguridad Vial.

Ng: Nanogramo (1ng = 1.0E-9 gr).

SV: Seguridad Vial.

OMS: Organización Mundial de la Salud.

ONSV: Observatorio Nacional de Seguridad Vial.

ONU: Organización de las Naciones Unidas.

SV: Seguridad Vial.

TC: Tribunal Constitucional.

UNE: Una Norma Española.

UE: Unión Europea.

1. INTRODUCCIÓN.

En el "Plan Mundial - Decenio de acción para la Seguridad Vial[1] 2021-2030" de la Organización Mundial de la Salud (OMS-ONU) se ha determinado que, uno de los principales comportamientos que contribuyen a los fallecimientos y a las víctimas por siniestros viales, es la conducción bajo los efectos del alcohol. Por ello, la OMS insta a los gobiernos a: diseñar el funcionamiento de un sistema de transporte por carretera seguro a través de la creación de leyes de Seguridad Vial (SV), a la aplicación de estas leyes y a promover la educación vial. Además, este organismo de la ONU no solo apremia a los organismos oficiales, también insta a las empresas privadas para que aborden y mitiguen las acciones que afectan negativamente a la SV y la difusión del mensaje de que un elevado consumo de alcohol y otras sustancias, como las drogas, contribuye a una "conducción peligrosa". También la OMS, se marca como meta para el año 2030 dos objetivos: reducir a la mitad el número de fallecidos y víctimas por siniestros viales causados por conductores bajo los efectos del alcohol y además, lograr una reducción de aquellos siniestros que sean ocasionados por el consumo de sustancias psicoactivas.

En relación con lo anterior, en España, el Observatorio Nacional de Seguridad Vial (ONSV)[2] como organismo dependiente del Ministerio del Interior y gestionado a través de la Dirección General de Tráfico (DGT), ha publicado la denominada "Revisión sistemática sobre drogas y conducción (2021)". Este documento nos remite a la "Ley sobre Tráfico, Circulación de Vehículos a Motor y Seguridad Vial " (LSV)[3], y en concreto a su Art. 14, que prohíbe la conducción con presencia[4] de drogas en el organismo (quedando excluidas aquellas sustancias que se utilicen bajo prescripción facultativa y con una finalidad terapéutica). Sin embargo, en este apartado de la LSV el legislador advierte que "(…) siempre que (el conductor) esté en condiciones de utilizar el vehículo conforme a la obligación de diligencia, precaución y no distracción[5] establecida en el Art.10".

Pero es que además, en España la conducción de vehículos a motor "bajo la influencia de drogas tóxicas, estupefacientes o sustancias psicotrópicas" puede suponer un delito contra la SV tipificado en el artículo 379.2 de la Ley Orgánica 10/2015 del Código Penal (CP). Por este motivo, el 17 de julio de 2019, la Fiscalía General del Estado (FGE) a través del Fiscal de Sala Coordinador de Seguridad Vial (FSCSV) emitió una Instrucción para la elaboración de atestados por delitos de conducción bajo la influencia de las drogas tóxicas, estupefacientes y sustancias psicotrópicas del Art. 379.2 del CP. En esta Instrucción, se pone en valor la importancia del acta de signos externos para determinar la influencia de estas sustancias, ya que el legislador español no dispuso de

---

[1] Ver: https://www.who.int/es/publications/m/item/global-plan-for-the-decade-of-action-for-road-safety-2021-2030.

[2]Ver: https://www.interior.gob.es/opencms/es/el-ministerio/funciones-y-estructura/subsecretaria-del-interior/direccion-general-de-trafico/

[3] Real Decreto Legislativo 6/2015, de 30 de octubre, por el que se aprueba el texto refundido de la Ley sobre Tráfico, Circulación de Vehículos a Motor y Seguridad Vial del Interior. BOE núm. 261, de 31 de octubre de 2015 Referencia: BOE-A-2015-11722.

[4] Positivo en drogas: procederá formular denuncia por infracción del art 14.1. 5ª de la LSV por presencia de drogas (1000 Euros / 6 puntos)".

[5] El conductor debe utilizar el vehículo con la diligencia, precaución y atención necesarias para evitar todo daño, propio o ajeno, cuidando de no poner en peligro, tanto a sí mismo como a los demás ocupantes del vehículo y al resto de usuarios de la vía, especialmente a aquellos cuyas características les hagan más vulnerables".

una tasa objetiva para determinar la afectación de las facultades psicofísicas del sujeto para una conducción segura, y por ello, el elemento típico de la influencia. Según sus propias palabras, "las tesis aplicadas al alcohol no son trasladables per se a las drogas tóxicas, estupefacientes y sustancias psicotrópicas, en las que las premisas científicas difieren del alcohol por diversas razones", y ello es debido a que no se ha conseguido establecer la influencia en las aptitudes psicofísicas del sujeto que le capacitan para una conducción segura, a partir de un nivel de concentración de droga detectada en un test salival.

Así, en nuestro país y según datos facilitados por la DGT[6] , "casi un tercio de los fallecidos por siniestro vial superaban el límite de alcoholemia", pero es que además, podemos afirmar desde la evidencia de la observación realizada durante más de dos décadas de ejercicio profesional "en carretera" del autor de este trabajo de investigación, que el estilo de vida de ocio y diversión nocturna es uno de los factores que aumentan la probabilidad de consumir alcohol y drogas (cannabis, cocaína y éxtasis) por parte de algunos conductores (Calafat, A. et al, 2000). Y que este consumo, se ha consolidado cada vez más en los últimos años, convirtiéndose en uno de los factores de riesgo más importantes de la siniestralidad vial en España.

También podemos afirmar, gracias a la experiencia profesional del autor, que otro factor de riesgo es circular como pasajero en un vehículo a motor cuyo conductor ha consumido alcohol o drogas, lo que ocasiona cada año un goteo constante de lo que podemos denominar "víctimas inocentes" (pasajeros, motoristas, peatones y ciclistas) que fallecen en siniestros viales como consecuencia de un conductor que circula bajo los efectos del alcohol o la influencia de las drogas, eso sí, tras una participación conjunta de ambos (conductor y pasajero) en las actividades nocturnas asociadas al ocio.

Es por lo que, a pesar de las políticas de SV de la DGT, de sus campañas de concienciación sobre el consumo de alcohol o drogas previo a la conducción, y de las campañas de vigilancia y control realizadas por los Agentes encargados de la vigilancia del tráfico, todavía no existe una verdadera "conciencia de SV comunitaria" o una "conciencia social vial" que nos haga comprender la peligrosidad de este tipo de conductas, pero sobre todo de llegar prevenirlas y en todo caso, como ocupantes o usuarios, rechazarlas y denunciarlas.

Finalmente, tenemos la obligación de mencionar aquellos conductores reincidentes o multirreincidentes (calificados así en función del tiempo transcurrido entre la comisión de una infracción y otra y del número de estas) y que al ser consumidores habituales de alcohol o drogas (o de ambas sustancias a la vez) pudieran denominarse "conductores adictos", y que se pueden considerar como potencialmente peligrosos para la SV y por ello, deben ser objeto de especial seguimiento y tratamiento como pacientes por las autoridades sanitarias[7], en coordinación con las labores de vigilancia y control por parte de la DGT .

---

[6]Ver: https://revista.dgt.es/es/noticias/nacional/2022/04ABRIL/0404_Campana-alcohol-Cifal.shtml.

[7]La normativa nacional RD 818/2009 Reglamento General de Conductores y la norma europea CD 439/1991, CD 126/2006 y CD 36/2012, señala que a estos pacientes (adictos) no se les puede otorgar o renovar el permiso de conducción ya que no presentan aptitudes adecuadas para una conducción segura.

2. LA ESTRATEGIA DE LA DIRECCIÓN GENERAL DE TRÁFICO: "TOLERANCIA CERO".

En junio del 2012 la DGT adoptó la medida de "tolerancia cero" como línea principal de estrategia sobre la conducción y el consumo de drogas, aplicando esta "tolerancia cero" a todos los conductores que consuman drogas y que se pongan a los mandos de un vehículo. Los motivos alegados por la DGT[8] eran que: "España se encuentra entre los países con mayor consumo de droga, especialmente la cocaína y el cannabis lo que produce como resultado el incremento del riesgo de sufrir siniestros viales y lesiones mortales o graves".

Así, según el estudio del Observatorio Europeo de las Drogas y Toxicomanías (EMCDDA[9] – "European Monitoring Centre for Drug and Drug Addiction") del año 2017, en la franja de edad de 15 a 34 años, España es:

El sexto país de la UE con mayor tasa de consumo de cocaína (con una prevalencia del 2,8%), tras el Reino Unido (4,7%), Holanda (4,5%), Dinamarca (3,9%), Francia (3,2%) e Irlanda (2,9%).

El cuarto país de la UE con mayor tasa de consumo de cannabis (18,3%), por detrás de Francia (21,8%), Italia (20,9%) y República Checa (19,3%).

Por ello, entre las acciones a emprender por parte de la DGT, y según su estrategia de "tolerancia cero" se enumeraban las siguientes:

Aumentar la sensibilización de toda la sociedad en torno al problema, informar a los conductores del riesgo del consumo de drogas (sin olvidar el riesgo que supone el consumo de alcohol), conocer cuáles son los consumos mínimos de alcohol y de drogas que provocan grandes deterioros para conducir, extender los controles de drogas y de alcohol + drogas en todo tipo de vías, días y horas; colaborar con otras administraciones en materia legislativa, educativa y formativa relacionada con las drogas y la conducción de vehículos, e impulsar la investigación aplicada en materia de drogas y seguridad vial.

Asimismo, y como objetivo para el año 2030, el Área estratégica de vigilancia y control de la DGT ha extendido la "tolerancia cero" a los comportamientos de riesgo que tienen mayor incidencia en los siniestros viales, marcando como ejes prioritarios: actuar sobre los excesos de velocidad, sobre el consumo de alcohol y drogas, uso del teléfono móvil durante la conducción y no hacer uso del equipamiento de seguridad (cinturón de seguridad, casco, sistemas de retención infantil, etc.).

[8]Documento "Drogas y conducción – Tolerancia Cero" (DGT).
https://www.interior.gob.es/opencms/pdf/prensa/balances-e-informes/2012/Presentacion-Tolerancia-cero-con-los-conductores-que-consuman-drogas-al-volante.pdf
[9]Ver: https://www.euda.europa.eu/publications_en

2.1. FUNDAMENTACIÓN Y PROCEDIMIENTO PARA LA REALIZACIÓN DE LA PRUEBA SALIVAL DE DROGAS.

Hasta hace relativamente poco, y debido a la carencia de Dispositivos Electrónicos de Detección portátiles (DED) con la tecnología adecuada, no era frecuente que "en carretera", se realizasen pruebas para detectar si el conductor había consumido drogas. El motivo es que, únicamente realizando un análisis de sangre se podía estar seguro de los resultados, pero, además, realizar estas pruebas en sangre y su posterior traslado a laboratorio para análisis, era relativamente complejo y de difícil encaje legal.

Posteriormente, la importancia del tema y el empeño de la DGT en detectar el consumo reciente de drogas y la presencia de estas en el organismo del conductor, pasó a ser muy relevante tanto para la SV, como para el entorno laboral del conductor profesional. Poco a poco, se implementaron los controles de drogas con dispositivos DED[10] portátiles que permiten detectar y analizar el consumo reciente de drogas en la saliva del conductor. A través de la obtención rápida de muestras de fluido bucal (como procedimiento no invasivo), se puede obtener un "positivo indiciario[11]" de consumo reciente de cinco drogas (anfetaminas, metanfetaminas, opiáceos, cannabis y cocaína). Sin embargo, se exige recoger una segunda muestra de saliva, denominada "prueba evidencial", cuyo objetivo es denominar y cuantificar el tipo de droga detectada en esta segunda muestra, y así confirmar el "positivo indiciario" obtenido; este segundo análisis salival se realizará en un laboratorio de referencia. El traslado al laboratorio de esta "prueba evidencial" se hace en un "tubo colector salival" precintado e identificado con un código de barras, que se introduce dentro de una nevera, previa reseña de éste en un documento que se rige por un estricto protocolo de cadena de custodia.

La obligatoriedad de esta prueba de laboratorio complementaria (prueba evidencial) tras el control inicial (prueba indiciaria) y la ratificación en el laboratorio de referencia del tipo de droga detectada y su cantidad, darán presunción de veracidad legal a la infracción por presencia de drogas en el organismo del conductor, así como la correspondiente apertura de un expediente administrativo sancionador por parte de la DGT.

3. LA DOCTRINA DE LA FISCALÍA GENERAL DEL ESTADO TRAS EL "POSITIVO" SALIVAL INDICIARIO EN DROGAS.

Según la doctrina de la Fiscalía General del Estado (FGE)[12], y una vez que ha resultado "positivo[13]" en el test indiciario salival que se ha realizado en un DED portátil que es capaz de analizar el fluido oral, resulta obligatorio el análisis posterior de la saliva en un "laboratorio homologado", dependiendo para ello de las necesarias actividades de control

[10] Ver: https://www.toxicology.abbott/es/es/screening-devices/sotoxa-mobile-test-system.html

[11] Se llama muestra "indiciaria" y detecta la posible **presencia** de sustancias ilegales. Ver: https://revista.dgt.es/es/sabia-que/normas/2018/0703como-se-hace-un-control-de-drogas.shtml

[12] Circular 10/2011 de 17 de noviembre (BOE FIS-C-2001-000010).

[13] La expresión, "positivo", no indica una determinada tasa en nanogramos, sino a cualquier resultado del que se desprenda la mera presencia de drogas en el organismo, es decir, no es una prueba cuantitativa, sino una prueba calificativa cuyo resultado es positivo o negativo.

por parte de Administración competente, garantizando además la "cadena de custodia[14]" de la saliva recogida para su análisis para afianzar la legalidad del procedimiento de obtención de las muestras salivales y convertirlas posteriormente en pruebas de cargo. También especifica la FGE, que los agentes encargados de la vigilancia del tráfico han de recibir una formación específica para su realización, ya que este tipo de pruebas son más complejas que las de detección alcohólica.

Una vez en el laboratorio, las muestras salivares son procesadas por equipos analíticos formados por un cromatógrafo de gases [15] (capaz de vaporizar substancias de volatilidades diferentes) y un espectrómetro de masas[16] (capaz de originar iones a partir de unas moléculas neutras en fase gaseosa, de separarlos en función de su masa y de detectarlos registrando la información adecuadamente), determinando qué tipo de droga y qué cantidad hay en la muestra salival. Estos equipos son capaces de detectar hasta cuarenta tipos de droga y de cantidades tan pequeñas como un nanogramo [17] (ng). Posteriormente, estos resultados de laboratorio son revisados uno a uno por personal facultativo especializado, quienes firman y validan el informe final para su envío a la DGT.

Sin embargo, como ya hemos indicado, a diferencia de las pruebas de alcohol, en el caso de las drogas tóxicas se ha adoptado una política de SV de "tolerancia cero", ya que la LSV [18] prohíbe de manera expresa y tácita la presencia de sustancias estupefacientes en el organismo del conductor. Una política vial no exenta de críticas, ya que diversos autores, reprochan que existe discrepancia entre los resultados positivos detectados en los DED y los resultados positivos del laboratorio (Ramírez, J, 2024).

Estos autores manifiestan que no se pueden contrastar los "cutoff" (puntos de corte analítico determinado en ng/ml)[19], de las marcas comercializadoras de los DED portátiles, ni los límites de detección confirmados por el laboratorio y tampoco la cantidad de la sustancia psicoactiva detectada

4. PRESENCIA DE DROGAS EN EL ORGANISMO: LA SANCIÓN ADMINISTRATIVA Y LA DOCTRINA DEL TRIBUNAL CONSTITUCIONAL.

La LSV sanciona administrativamente con la detracción de 6 puntos y 1000 euros de multa al que conduzca con presencia de drogas en el organismo. En este punto haremos

[14] Se entiende por cadena de custodia el proceso mediante el que se acredita que el objeto incautado es el mismo que finalmente ha sido analizado. La posible rotura de la cadena de custodia podría dar lugar a la vulneración del derecho a un proceso con todas las garantías.

[15]Ver:https://www.mncn.csic.es/docs/repositorio/es_ES/investigacion/cromatografia/espectrometria_de_masas.pdf

[16]Universidad de la Rioja. Servicio de Laboratorio y Talleres**.** Cromatografía de Gases**:** Análisis cualitativo por cromatografía de gases detección de masas Sin operaciones previas de preparación de muestra. 75 € / hora. Espectrometría de masas: Análisis cualitativo por espectrometría de masas electrospray/alta resolución Sin operaciones previas de preparación de muestra. 120 € / hora.

[17] Milmillonésima parte de un gramo:1 ng. = 1e-9 gr.

[18] RD 6/2015 de 30 de octubre, modificada Ley 18/20221 de 20 diciembre BOE núm. 304. Un "cutoff" o punto de corte, es la concentración de una sustancia a partir de la cual una prueba diagnóstica se considera positiva.

[19] Un *"cutoff"* o punto de corte, es la concentración de una sustancia a partir de la cual una prueba diagnóstica se considera positiva.

mención al Pleno 174/2017 del Tribunal Constitucional[20](TC), debido a la cuestión de inconstitucionalidad planteada en relación a varios artículos del RD 339/1990[21] , y en concreto sobre la pertinencia de plantear cuestión de inconstitucionalidad en relación con el Art. 12 de la Ley 6/2015, al tipificar como infracción administrativa conducir un vehículo "con presencia de drogas en su organismo", sin que sea necesario acreditar que la presencia de esas drogas haya influido en sus capacidades para conducir. El Alto Tribunal "no aprecia que los preceptos cuestionados sean inconstitucionales por prohibir el consumo de drogas, a través de una Norma que tiene como finalidad proteger la SV". Aclara además, que los preceptos cuestionados "no tienen como objeto prohibir en general el consumo de drogas". Por lo tanto, lo que prohíbe es: Que los conductores conduzcan "con presencia de drogas en el organismo (…)". Así, se "tipifica como infracción administrativa, por lo que la conducta prohibida y constitutiva de infracción administrativa no es consumir drogas, sino conducir si se han consumido este tipo de sustancias". Pero lo que resulta aún más interesante, es que el Alto Tribunal equipara el consumo de drogas tóxicas, con el consumo de drogas bajo prescripción facultativa y con fines terapéuticos, ya que: "El riesgo que puede conllevar para la seguridad del tráfico conducir con presencia de este tipo de sustancias en el organismo será el mismo tanto en el caso de que las drogas consumidas se efectúen por indicación médica como en los supuestos en los que el consumo de estas no tenga finalidad terapéutica".

En consecuencia, el TC no aprecia que los preceptos cuestionados vulneren artículos constitucionales y que con ello se invalide el planteamiento y el concepto de lo que debe entenderse por "drogas", es más, garantiza que este concepto es el que define como aquella sustancia que tiene la entidad suficiente para alterar las capacidades psicofísicas de quien las consume, y que "La norma pretende al tipificar como infracción administrativa conducir con presencia en el organismo de drogas, es evitar que se conduzca si se han tomado sustancias que pueden alterar las condiciones psicofísicas para conducir, dado el riesgo que conducir en tales condiciones puede entrañar para la seguridad del tráfico (…)".

5. LOS PUNTOS DE CORTE Y LAS CANTIDADES MÍNIMAS PSICOACTIVAS.

De nuevo advierte la DGT, en el documento "Revisión sistemática sobre drogas conducción" (2021), que no hay acuerdos internacionales ni nacionales al respecto de los puntos de corte (cuantificados en ng /ml)[22] a establecer en los procedimientos de control del consumo de sustancias en los conductores y que España fue uno de los primeros países en regular la prueba mediante muestra de saliva. Para ello, la DGT dice haber tenido en cuenta los valores recomendados a nivel internacional en materia de seguridad laboral, donde una serie de organismos de reconocido prestigio, la Substance Abuse and Mental Health Services Administration (SAMHSA) [23] en Estados Unidos, la European Workplace Drug Testing Society (EWDTS)[24], o la National Safety Council´s Alcohol, Drugs and Impairment Division (NSC-ADID)[25] de Europa y Reino Unido), han emitido

[20] BOE núm. 15 de 17 de enero de 2018. Sec. TC.
[21] BOE núm. 63 de 14 de marzo de 1990 por el que se aprueba el articulado de la Ley sobre Tráfico, Circulación de Vehículos a motor y Seguridad Vial.
[22] Nanogramo (ng): Es una unidad de medida de masa que corresponde a la milmillonésima parte de un gramo.
[23] Ver: https://www.samhsa.gov
[24] Ver: http://www.ewdts.org
[25] Ver: https://www.nsc.org/workplace/get-involved/divisions/alcohol-drugs-impairment-division

informes actualizados sobre las recomendaciones de los puntos de corte que se deben establecer, ajustándose además a los requerimientos de las normas ISO[26] /IEC[27] en el caso europeo.

Así, basándonos en lo anterior, el Ministerio del Interior estableció unos valores de positividad para el análisis evidencial en el laboratorio publicados en el documento "Revisión sistemática sobre drogas conducción" (2021). Tanto es así que la DGT dice ajustar estos valores a las recomendaciones más recientes y aplicables en el ámbito internacional, y además, a la evidencia generada por la experiencia española en este campo.

5.1. TABLA 1.

Comparativa de los puntos de corte analítico para la prueba evidencial en fluido oral del consumo de sustancias psicoactivas en conductores de la dirección general de tráfico y otros organismos internacionales.

ANALITO	Cutoff saliva (ng/ml)			
	EWDTS	SAMSHA	NSC-ADID	**DGT**
Anfetamina	15	15	15	**15**
Cocaína	8	8	8	**8**
Ketamina	10			**10**
MDA	15	15	15	**15**
MDEA	15	15		**15**
MDMA	15	15	15	**15**
Metadona	20		10	**10**
Metanfetamina	15	15	15	**15**
Morfina	15	15	5	**5**
THC	2	2	2	**2**

Fuente: Elaboración propia según DGT (2021).
"Revisión sistemática sobre drogas y conducción"

Nota: EWDTS: European Workplace Drug Testing Society (UK).
SAMHSA: Substance Abuse and Mental Healt Service Administration (USA).
NSSC-ADID: National Safety Council - Alcohol, Drugs and Imparment Division (USA).

Análisis comparativo de los límites de detección (cutoff) de los analitos de la tabla 1:

5.1.1 Consenso Internacional: Los analitos como la anfetamina, metanfetamina, MDMA, MDA, cocaína y THC presentan unos valores homogéneos (15 ng/ml para los estimulantes; 8 ng/ml para cocaína y 2 ng/ml para el THC, lo que demuestra que los estándares son ampliamente aceptados para su detección.

[26] Real Academia Española: Organización Internacional de Estandarización, es el sistema de normalización internacional para la regulación de los productos y servicios.
[27] Comisión Electrotécnica Internacional, es la comisión de normalización líder en el mundo que desarrolla y publica estándares internacionales para las tecnologías electrónicas.

5.1.2. Variabilidad en analitos específicos: La metadona y la morfina muestran límites más bajos en NSC-ADID y DGT, lo que indican que existen criterios más sensibles, posiblemente por razones forenses y de seguridad vial.

5.1.3. Tendencia del estándar DGT: La normativa española de la DGT incluye todos los analitos relevantes, pero además, adopta límites más estrictos en algunos casos, lo que viene a indicar una priorización de la detección precoz con fines preventivos administrativos y también penales.

5.2. TABLA 2.

Comparativa de puntos de corte (positivo): DED Sotoxa[28], laboratorio SynLab y los establecidos por la DGT.

ANALITO	ABBOT SOTOXA[29] TOX400SEU	SYNLAB Laboratorio SYNLAB[30]	DGT DGT[31]
6-AM (morfina) (OPI)[32]	40 ng/ml	>2,6 ng/ml	2 ng/ml
Anfetamina (AMP)	**50 ng/ml**	>18,8 ng/ml	15 ng/ml
Benzoilecgonina (BE)	30 ng/ml	>9,9 ng/ml	8 ng/ml
Metabolito de cocaína (COC)	**30 ng/ml**	>10 ng/ml	8 ng/ml
Codeína (OPI)	**40 ng/ml**	>12,2 ng/ml	5 ng/ml
Ketamina		>12,6 ng/ml	10 ng/ml
MDA	50 ng/ml	>18,3 ng/ml	15 ng/ml
MDEA	50 ng/ml	>18,2 ng/ml	15 ng/ml
Metanfetamina (MDMA)	**50 ng/ml**	>18,7 ng/ml	15 ng/ml
Metadona (OPI)	**40 ng/ml**	>12,2 ng/ml	10 ng/ml
Morfina (OPI)	**40 ng/ml**	>6,2 ng/ml	5 ng/ml
Cannabis (THC)	**25 ng/ml**	>2,5 ng/ml	2 ng/ml

Fuente: Elaboración propia (2023); según informes de la comercial SYNLAB, de monitorización de fármacos y toxicología.

Observaciones clave de la tabla 2:

5.2.1 SOTOXA (DED). Muestra los valores más altos y refleja puntos de corte para dar positivo más permisivos, no una concentración real.

5.2.2. SYNLAB. Informa sobre valores reales superiores a un mínimo detectable y reporta resultados cuantitativos por encima de un umbral, pero no normativos.

---

[28] Ver: ANEXO I. Explica la "composición y principios de funcionamiento del analizador Abbot-SoToxa".
[29] Ver: https://www.toxicology.abbott/es/es/screening-devices/sotoxa-mobile-test-system.html
[30] Extraído del informe de ensayo confirmatorio de drogas en saliva por LC-MS/MS del laboratorio SYNLAB.
[31] DGT (2021); "Revisión sistemática sobre drogas conducción" (2021).
[32] OPI: Opiáceos.

5.1.3. DGT. Proporciona los valores más bajos, y son umbrales de corte legales de confirmación toxicológica, estableciendo los límites legales de la infracción administrativa y la correspondiente sanción.

6. LA EMPRESA DE ANÁLISIS CLÍNICOS SYNLAB.

"Cualquier prueba, en cualquier lugar, en cualquier momento", ese es el lema de la empresa alemana Synlab Group (SYNLAB)[33].

SYNLAB fue fundada en 1998 por el doctor Bartl Wimmer en Augsburgo, junto con un grupo de socios como una asociación de médicos de laboratorio independientes. Desde entonces ha crecido principalmente mediante adquisiciones, ofreciendo durante la pandemia los test para detectar la presencia del coronavirus. SYNLAB no ha pasado desapercibida entre los grandes inversores institucionales a nivel mundial, que a lo largo de estos años han entrado en el capital social. Actualmente el principal accionista es el conocido fondo de capital riesgo británico Cinven (con oficina también en Madrid), que ostenta en torno al 43% de las acciones, según las estimaciones de la alemana. A continuación aparecen los daneses de Novo Holdings (17%); los canadienses del fondo de pensiones de los maestros de Ontario (OTPP) con el 8%; idéntico porcentaje que el fundador de SYNLAB y sus allegados; y el Estado de Qatar a través de su fondo soberano (5%).

En España, su relación con el Ministerio del Interior (según la plataforma de contratación del Sector Público del Ministerio de Hacienda), se ha fraguado a través de la DGT, quien ha licitado el "servicio de determinación y cuantificación de drogas y alcohol en muestras de fluido oral y de sangre" en base a un contrato[34] adjudicado por un valor de 4.999.980,00 Euros a SYNLAB DIAGNÓSTICOS GLOBALES S.A.U (A59845875). Además de la DGT, este laboratorio clínico ha realizado contrataciones con más administraciones: la Junta de Andalucía en materia de análisis clínicos para el Centro de Prevención de riesgos laborales de Jaén, con el Metro de Madrid o con la Generalidad de Cataluña[35] entre otros.

7. LÍMITES DE CUANTIFICACIÓN Y RANGOS DE INCERTIDUMBRE EN LOS RESULTADOS DEL LABORATORIO SYNLAB.

Existe una información adicional de las muestras de saliva remitidas por el laboratorio SYNLAB de las sustancias anteriormente citadas en la tabla; se utiliza como "criterio de positividad" que la concentración de las sustancias sea superior o igual a los valores del límite de cuantificación (LPC)[36], más el "valor de incertidumbre" del ensayo, en caso contrario, el resultado es negativo. Además, SYNLAB alude a que su laboratorio dispone de "la incertidumbre expandida para K=2 de todo el rango de trabajo".

---

[33] Ver: https://valenciaplaza.com/asi-es-synlab-empresa-alemana-compra-sistemas-genomicos

[34] Ver:https://contrataciondelestado.es/wps/portal/!ut/p/b0/04_Sj9CPykssy0xPLMnMz0vMAfIjU1JTC3Iy87KtUlJLEnNyUuNzMpMzSxKTgQr0w_Wj9KMyU1zLcvQj_byycwN9yy2dXPLygvNDIoyrVA3Myx1tbfULcnMdAUNYE4U!/ y BOE 97 de 23 de abril de 2019.

[35] Ver: https://contractaciopublica.cat/ca/detall-publicacio/200026255

[36] Es el término con el que se hace referencia a la concentración más baja que de una manera fiable se puede alcanzar, siempre y cuando esté dentro de los límites de precisión especificados en el funcionamiento rutinario del laboratorio.

Para aclarar el concepto de "incertidumbre", debemos decir que es la "duda" que puede existir sobre el resultado de cualquier medición, es decir, nos viene a decir la fiabilidad de esa medida.

Por ello, todas las mediciones que se hacen tienen algo de "duda" y se debe cuantificar para decidir si la medida realizada es lo suficientemente fiable para el propósito que se ha requerido. Además, debemos puntualizar que, "error" no es lo mismo que "incertidumbre*",* a saber:

Error: Es la diferencia entre el valor de la medida de un equipo y el patrón o valor de referencia[37] que es tomado como exacto. Al realizar una comparación entre valores, se genera error e incertidumbre según la metrología. De tal forma que, juntos error e incertidumbre, se pueden utilizar para saber si un instrumento está dentro del error máximo tolerado.

Incertidumbre[38]: Tras realizar varias mediciones durante un proceso de calibración, se descubren pequeñas diferencias entre ellas. Pero, ¿cuál medición es la correcta?, pues se halla la media y su desviación estándar, averiguando cuál es la diferencia normal entre las mediciones, haciendo que la medida final sea lo suficientemente fiable.

Exactitud: Mide el grado de concordancia entre el resultado obtenido y el valor verdadero (o el tomado como tal).

Precisión: Muestra la concordancia entre dos o más medidas que han sido tomadas de la misma manera

Incertidumbre expandida [39] : Antes de publicar la componente de incertidumbre combinada, es necesario multiplicar el resultado por el valor sigma seleccionado para obtener el nivel de confianza requerido. Después de hacer la multiplicación, lo que se obtiene es la incertidumbre expandida, es decir, la incertidumbre con un nivel de confianza determinado incluido.

Evaluación de la incertidumbre K=2: La calibración se realiza por un laboratorio autorizado (calibración externa) y los datos de incertidumbre expandida se indican en %, siendo K=2 correspondiente aproximadamente a un nivel de confianza del 95 %.

Por lo tanto, podemos afirmar que los resultados analíticos salivares de drogas del laboratorio SYNLAB, tienen un nivel de confianza o de precisión esperada que los sitúa en torno al rango/límite del 95 %.

---

[37] Patrón, con la mayor exactitud disponible en un lugar o en una organización determinada, y del cual se derivan las mediciones.

[38] NSGT (2012) Incertidumbre del resultado de una medición, expresada en forma de una desviación típica experimental. Ver: https://www.insst.es/documents/94886/326879/930w.pdf/f657c677-ebab-4f99-8474-667d73e22882

[39]INSGT (2012): Magnitud que define un intervalo en torno al resultado de una medición, y en el que se espera encontrar una fracción importante de la distribución de valores que podrían ser atribuidos razonablemente al mensurando.

8. EL LABORATORIO SYNLAB Y SU HOMOLOGACIÓN POR LA ENTIDAD NACIONAL DE ACREDITACIÓN MEDIANTE AUDITORÍAS.

La Entidad Nacional de Acreditación (ENAC G-78373214 – C/Serrano 240, 4ª A-B, 28016 Madrid)) es el único organismo designado por el Gobierno, para operar en España como Organismo Nacional de Acreditación[40] , regulando el funcionamiento de la acreditación en Europa, que se basa en cinco principios fundamentales: "Ausencia de ánimo de lucro, independencia, no competencia, evaluación internacional y reconocimiento mutuo[41] ". Además, el organismo ENAC puede firmar con la Administración General del Estado y con las Administraciones de las Comunidades Autónomas los convenios de colaboración que resulten pertinentes para el mejor desempeño de sus actividades y funciones[42].

La "acreditación" de ENAC debería ser una garantía de correcta ejecución de un determinado tipo de actividades, a través de un certificado que esta entidad emite.

A modo de ejemplo, ENAC ha realizado las siguientes actividades:

Año 2013, ha acreditado al Instituto de Salud Carlos III[43] de Investigación en enfermedades raras según la norma UNE-En ISO 15189 para la realización de análisis.

Año 2016, "auditoría externa de acreditación de ensayos y de actividades de inspección técnico ocular" de los laboratorios de criminalística de la Guardia Civil[44].

Año 2018, ha realizado "servicios de auditoría" en la Universidad de A Coruña[45].

Año 2022, ha acreditado[46] a la Policía Científica del Cuerpo nacional de Policía para la "realización de inspecciones técnico-policiales en la escena del delito", conforme a la norma ISO 17020.

Año 2023, ha realizado "actividades de acreditación encaminadas a la evaluación de los laboratorios" de la Universidad Complutense de Madrid[47].

Por otra parte, en relación con las actividades de un laboratorio privado (como SYNLAB), pueden ser: de ensayo, de calibración, inspección, entidades de certificación o verificación entre otras, sin embargo, cualquier actividad que tenga por objeto evaluar

---

[40] RD 1715/2010 BOE 7 de núm. 7 de 8 de enero de 2011, "(…) de acuerdo con lo establecido en el Reglamento (CE) N.º 765/2008 del Parlamento Europeo y el Consejo, de 9 de julio de 2008, por el que se establecen los requisitos de acreditación y vigilancia del mercado relativos a la comercialización de los productos y por el que se deroga el Reglamento (CEE) Nº.: 339/93.

[41] Ver: *https://www.innotec-laboratorios.es/que-es-la-acreditacion-enac/*

[42] BOE núm. 7, de 8 de enero de 2011.

[43]Ver:https://www.isciii.es/QueHacemos/Servicios/DiagnosticoGenetico/Documents/ACREDITACION_SDG_IIER_sin_anexo_tecnico.pdf

[44]Ver:https://www.isciii.es/QueHacemos/Servicios/DiagnosticoGenetico/Documents/ACREDITACION_SDG_IIER_sin_anexo_tecnico.pdf

[45]Ver: https://www.udc.es/export/sites/udc/contratacionadministrativa/contratos-menores/publicar-Disp-adic-54.xls_2063069239.xls

[46] Ver: https://www.enac.es/actualidad/policia-cientifica-inspeccion-ocular

[47] Ver: [47] https://www.ucm.es/file/208-2023-enac-1-

si un producto, servicio, sistema, instalación, etc. debe ser conforme a ciertos requisitos y puede estar sujeta a acreditación.

Estos requisitos pueden estar establecidos por ley y tener por tanto carácter reglamentario o estar legislados en normas, especificaciones u otros documentos de carácter voluntario. La acreditación de ENAC no solo ofrece a cualquier laboratorio o empresa evaluada la manera de saber si su actividad se está llevando a cabo correctamente, si no que, además, garantiza la máxima eficacia de sus servicios a los clientes de esos laboratorios.

Para evaluar la correcta actividad del laboratorio, se programan auditorías anuales de seguimiento y cada cuatro años una auditoría de reevaluación. En las auditorías de seguimiento se revisa si ha habido cambios en los procedimientos, adquirido nuevos equipos, etc.

En resumen, lo que ENAC puede evaluar y certificar es el correcto cumplimiento de la norma[48] UNE-EN ISO/IEC 17025 en ese año. A modo de información, en las auditorias de reevaluación se revisan más exhaustivamente todos los puntos de la norma durante los cuatro años anteriores. Si el laboratorio no cumple los requisitos en cualquiera de estas auditorías, la entidad podría suspender la acreditación.

A modo de información, en las auditorias de reevaluación se revisan más exhaustivamente todos los puntos de la norma durante los cuatro años anteriores. Si el laboratorio no cumple los requisitos en cualquiera de estas auditorías, la entidad podría suspender la acreditación.

[48] BOE 19 de 22 de enero de 2018 – Ministerio de Economía, Industria y Competitividad por la que se publican los "Requisitos generales para la competencia de los laboratorios de ensayo y calibración. (ISO/IEC 17025:2017)".

9. TABLA 3. ALCANCE DE LA ACREDITACIÓN[49] ENAC Nº 1169/LE2347, EXPEDIDA A LOS LABORATORIOS SYNLAB DIAGNÓSTICOS GLOBALES SA., SOBRE LOS ENSAYOS (REVISADO EL 23/12/2022).

ENTIDAD NACIONAL DE ACREDITACIÓN (ENAC)

PRODUCTO/ MATERIAL A ENSAYAR *PRODUCTS/MATERIALS TESTED*	**ENSAYO** *TYPE OF TEST*	**NORMA / PROCEDIMIENTO DE ENSAYO** *STANDARD SPECIFICATIONS/ TEST PROCEDURE*
Saliva (directa o saliva en tampón) Sangre total *Saliva (direct or saliva in buffer)* *Blood*	Determinación cuantitativa de sustancias de abuso mediante cromatografía líquida ultrarrápida de alta resolución con detección de espectrometría de masas en tándem.	Procedimiento interno LCMS-004 Rev.15 LCMS-0010 Rev.9

SUSTANCIA	LOQ[50] ng/ml Saliva	LOQ ng/ml Sangre
Morfina	**1**	**1**
Codeína	1	2
Heroína	**2**	**2**
Anfetamina	**1**	**2**
Metanfetamina	**1**	**2**
MDA	2	2
MDMA	2	2
MDEA	2	2
Cocaína	**1**	**2**
Metadona	**2**	**2**
Ketamina	2	2
LSD	2	2
Clonazepam	2	2
Alprazolam	2	2
Diazepam	1	2
Lorazepam	2	2
Oxazepam	2	2
Nordiazepam	1	2
Tramadol	1	2
Fenciclidina	2	2
Dextropropoxifeno	1	2
Zolpidem	1	2

ENAC
CALIBRACIÓN ISO 17025 Nº62 / LC10.039

Fuente: SYNLAB (Elaboración propia)

[49]Ver:https://synlab.es/fileadmin/user_upload/Calidad_docs/Anexo_Tecnico_ISO_17025_version_7.pdf
[50] LOQ: Límite de cuantificación o nivel más bajo. en inglés, "Limito Of Quantification".

OBSERVACIONES CLAVE DE LA TABLA 3:

9.1. MAYOR SENSIBILIDAD EN SALIVA.

En quince de las veintidós sustancias de la tabla, el LOQ en saliva es inferior al de sangre, lo que destaca la eficacia de esta matriz para detección temprana de la sustancia.

9.2. IGUAL SENSIBILIDAD EN MATRICES PARA CIERTOS COMPUESTOS.

Siete sustancias (p. ej., LSD, ketamina, benzodiacepinas) tienen el mismo LOQ en ambas matrices (2 ng/ml), esto indica que la matriz no afecta significativamente la sensibilidad analítica para estos compuestos.

9.3. POSIBLES IMPLICACIONES CLÍNICAS Y FORENSES.

La saliva se ha consolidado como una alternativa no invasiva y altamente sensible para el análisis toxicológico, de tal forma que, el menor LOQ en saliva favorece su uso en escenarios como: puntos de verificación de drogas, programas de deshabituación o monitorización laboral, donde el acceso a un análisis de sangre puede ser limitado y poco operativo.

9.4. ANÁLISIS SALIVAL VS ANÁLISIS DE SANGRE.

La saliva se ha posicionado como una matriz de alto valor en la toxicología analítica, no solo por su menor invasividad, sino también por su capacidad para ofrecer mayores niveles de sensibilidad de detección rápida de consumo reciente.

La detección temprana es especialmente relevante en situaciones de prevención y control en tiempo real, tanto en los puntos de verificación de drogas, como en siniestros viales en los que se encuentre implicado un conductor bajo la posible influencia de estas sustancias.

El uso de la saliva, en combinación con el análisis de laboratorio, representa una herramienta analítica eficaz y de sensibilidad superior a la de la sangre. Todo ello en términos de límite de cuantificación para un amplio espectro de sustancias de abuso.

La recomendación de la incorporación de los análisis salivales, como matriz de referencia en protocolos de detección temprana y diagnóstico toxicológico moderno, ha resultado acertada.

10. CONCLUSIONES.

Primero. La ONU insta a gobiernos e instituciones (públicas y privadas), a través del cumplimiento de las leyes de SV, a que logren la reducción de los siniestros viales mortales ocasionados por el consumo de drogas.

Segundo. En España, la DGT (Ministerio del Interior), ha instaurado una política de "tolerancia cero" al volante, calificando como conducta de riesgo, la conducción con presencia de drogas en el organismo. Esta conducta se castiga siempre, bien como infracción administrativa o bien como delito penal.

Tercero. A pesar de no existir acuerdos internacionales sobre los "puntos de corte", la DGT ha establecido los "cutoff" de las cantidades mínimas psicoactiva. Estas cantidades, se homologan a las de organizaciones públicas y privadas tanto de la UE como de USA. Con ello, la DGT ha determinado la positividad cuantitativa de cualquier droga consumida recientemente por un conductor y que posteriormente, será analizada en el laboratorio de referencia.

Cuarto. La doctrina de la FGE avala el procedimiento de recogida de muestras salivales tras el test indiciario positivo, a través de: la formación específica de los agentes en la recogida de la muestra, la garantía de la cadena de custodia y de un posterior análisis salival en un laboratorio de referencia.

Quinto. El TC avala el Art. 14 de la LSV, aclarando que, la Ley no prohíbe el consumo de drogas; lo que prohíbe es conducir con presencia de drogas en el organismo.

Sexto. El TC equipara y pone al mismo nivel, el riesgo que puede generar para la SV aquel conductor que haya consumido drogas, incluso las ingeridas bajo prescripción médica.

Séptimo. Los "puntos de corte" de los DED portátiles (SoToxa Abbott) utilizados para realizar la primera "prueba indiciaria", duplican o triplican los "puntos de corte" de referencia realizados laboratorio SYNLAB.

Octavo. Los "puntos de corte" del laboratorio clínico SYNLAB, son más altos que los que determina la norma ISO, y que la DGT aplica para establecer como cantidades mínimas psicoactivas en los equipos analizadores de laboratorio.

Noveno. La homologación del análisis clínico salival del laboratorio SYNLAB está avalada por la Entidad Nacional de Acreditación (ENAC), quien certifica el cumplimiento de la norma UNE de los equipos y el procedimiento utilizado por el laboratorio SYNLAB en la obtención de los diagnósticos salivales, tanto en el tipo de droga detectada como en su cantidad.

Décimo. La evaluación de los equipos y el procedimiento de obtención de los análisis de las muestras de saliva del laboratorio SYNLAB por parte de ENAC, acredita el 95% de nivel de confianza o de precisión de los resultados finales obtenidos y plasmados en su informe final.

11. REFERENCIAS.

Abbot. (2020). Analizador portátil de pruebas toxicológicas SoToxa. https://www.tecmedica.es/cmsAdmin/uploads/o_1f24002cp1ieo17701uni19v4vaja.pdf.

Abbot. (2020). Analizador portátil de fluido oral SoToxa (Manual de usuario). https://testdealcoholydrogas.cl/wp-content/uploads/2022/08/Manual-APOC0798-v2.a-SoToxa-Mobile-Analyser-User-Guide-FWO-LA.pdf

Asociación Española de Normalización. (2017). Requisitos generales para la competencia de los laboratorios de ensayo y calibración (ISO/IEC 17025:2017). https://www.une.org/

Bequir, S. (2020). Test de droga en saliva, ¿Cuánto dura? https://institutocastelao.com/test-de-droga-en-saliva/

Calafat, A et al. (2002). Vida recreativa nocturna de los jóvenes españoles como factor de riesgo frente a otros más tradicionales. https://www.redalyc.org/pdf/2891/289122037002.pdf

Certum Diagnostics. (2019). Pruebas de drogas (en orina). https://industriasquimicasybiologicas.com/wp-content/uploads/2020/09/Brochure-cassete-individualPrueba-de-Drogas-Certum_Kabla.pdf

Dirección General de Tráfico. (2021). Revisión sistemática sobre drogas y conducción. https://www.dgt.es/conoce-la-dgt/que-hacemos/conocimiento-e-investigacion/revision-sistematica-sobre-drogas-y-conduccion

Dirección General de Tráfico. (2022). Estrategia de seguridad vial 2030. https://seguridadvial2030.dgt.es/inicio/

Entidad Nacional de Acreditación (s.f.). Folleto ENAC institucional. https://www.enac.es/actualidad/material-multimedia

Entidad Nacional de Acreditación. (2022). Memoria 2022. https://www.enac.es/memoria-2022

Fiscalía General del Estado. (2021). Circular 10/2011 FGE, de 17 de noviembre, sobre criterios para la unidad de actuación especializada del Ministerio Fiscal en materia de seguridad vial. https://www.boe.es/buscar/doc.php?id=FIS-C-2011-00010

Instituto Nacional de Toxicología. (2021). Cuadro de dosis mínimas psicoactivas de las principales sustancias tóxicas objeto de tráfico de drogas. https://pnsd.sanidad.gob.es/ciudadanos/legislacion/delitos/pdf/20210730_INTF_dosis_minimas_psicoactivas_trafico_de_drogas.pdf

Observatorio Español de las Drogas y las Adicciones. (2023). Informe 2023 – Alcohol, tabaco y drogas ilegales en España.

https://pnsd.sanidad.gob.es/profesionales/sistemasInformacion/informesEstadisticas/pdf/2023OEDA-INFORME.pdf

Observatorio Nacional de Seguridad Vial. (2021). Revisión sistemática sobre drogas y conducción. https://www.dgt.es/conoce-la-dgt/que-hacemos/conocimiento-e-investigacion/revision-sistematica-sobre-drogas-y-conduccion

Organización Mundial de la Salud. (2021). Plan Mundial - Decenio de acción para la seguridad vial 2021-2030. https://www.who.int/es/publications/m/item/global-plan-for-the-decade-of-action-for-road-safety-2021-2030

Ortega Matus, M. (2022). Anticuerpos monoclonales y su empleo para identificar morfina en fluidos biológicos. https://riiad.org/index.php/riiad/article/view/riiad-2023-1-09/389

Parra, M. & Vega, V. (2021). Análisis de drogas de abuso en laboratorio clínico. https://www.seqc.es/download/tema/38/7601/85888673/142010/cms/tema-9-analisis-de-drogas-de-abuso-en-el-laboratorio-clinico.pdf/

Ramírez, J. (2024). Los controles de drogas a conductores en España. https://observatoriocannabis.com/wp-content/uploads/2024/10/controlesdedrogas.pdf

Ruiz Viera, L. (2018). Anticuerpos monoclonales terapéuticos. https://riull.ull.es/xmlui/bitstream/handle/915/12352/Anticuerpos+monoclonales+terapeuticos.pdf;jsessionid=3462A6DCEAB9DA8E32233B47C6D926E0?sequence=1

SGC-Laboratorios. (2023). Cómo evaluar la incertidumbre de medición sin ser un experto en matemáticas. https://sgc-lab.com/guia-para-estimar-la-incertidumbre-de-la-medicion-hecha-para-personas-normales/

ANEXO I

COMPOSICIÓN Y PRINCIPIOS DEL ANALIZADOR ABBOT-SOTOXA

1.1. COMPOSICIÓN[51].

El analizador Abbot SoToxa está formado por un sistema de analizador portátil (DED), un cartucho o kit de prueba y un dispositivo de obtención de fluido oral.

1.1.1. El analizador:

Es un dispositivo de análisis digital portátil de saliva, que usa algoritmos para determinar la intensidad de unas líneas de contraste (que aparecerán en la tira del cartucho de prueba tras todo el proceso) y que además, puede mostrar en una pantalla e imprimir los resultados cualitativos y nominativos de las drogas detectadas.

1.1.2. El cartucho de prueba:

Compuesto des una tira de inmunoensayo[52] cromatográfico[53] rápido de papel de un solo uso desechable, que contiene reactivos secos y una solución en tampón. Este kit se introduce en el analizador que lo calienta hasta la temperatura óptima para la realizar la prueba.

1.1.3. El dispositivo de obtención:

Es un dispositivo desechable que recoge el fluido oral (saliva). Debe frotarse con las encías, lengua e interior de las mejillas hasta que el indicador de presencia se coloree de azul.

1.2. PROCESO DE LA PRUEBA:

El fluido oral recogido en el dispositivo de obtención se combina con la solución del tampón, después, se mezcla y se incuba antes de ponerse en contacto con las tiras del inmunoensayo instaladas en el cartucho de prueba con *"una membrana con humedad controlada"*.

La mezcla de la solución y la saliva obtenida fluye por la capilaridad de la tira del cartucho y arrastra los anticuerpos antidroga marcados que se encuentran depositados en ella. En ausencia de droga en la muestra, el anticuerpo enlaza con la mezcla droga-proteína formando una línea. En presencia de droga la formación de esta línea más débil.

---

[51] Abbot (2020); "Analizador portátil de fluido oral SoToxa" (Manual de usuario).

[52] Se usa un inmunoensayo cromatográfico rápido para la detección cuantitativa de múltiples drogas y metabolitos de drogas en saliva, que proporciona solamente un resultado preliminar de la prueba analítica.

[53] La cromatografía es una técnica realizada en laboratorios para separar los componentes en mezclas simples o complejas. Hay muchos tipos diferentes de cromatografía, que van desde la cromatografía en papel y la cromatografía en capa fina hasta la cromatografía de gases.
Ver:https://www.onelab.com.ar/cromatografia-que-es-y-para-que-sirve-informacion-completa

Acto seguido el DED lee la intensidad de las líneas de la tira de inmunoensayo del cartucho y esta intensidad la compara con un umbral o punto de corte predeterminado de concentración de drogas, obteniendo un resultado cualitativo (no cuantitativo). Posteriormente, los resultados son mostrados en la pantalla del DED y pueden ser impresos.

1.3. RESULTADOS POSITIVOS.

El manual del DED Abbot SoToxa especifica que los resultados positivos obtenidos deben ser confirmados por un segundo método como puede ser la cromatografía de gases con espectrometría de masas (CGEM). Además, el DED y sus resultados no están diseñados para el uso doméstico, ni en entornos clínicos, terapéuticos o de diagnóstico.

1.4. COMPOSICIÓN DE LA TIRA DE INMUNOENSAYO DEL CARTUCHO.

El contenido de inmunoensayo cromático está compuesto por una tira que tiene impregnada una serie de reactivos secos que contienen anticuerpos monoclonales[54] (mAbs). Estos anticuerpos (AC) son proteínas creadas en laboratorio y se usan para identificar los metabolitos de drogas de abuso en fluidos biológicos.

Los mAbs tienen una alta sensibilidad y se adhieren por ejemplo, a la morfina y a sus metabolitos, por lo que se pueden ser usados para generar un resultado marcado mediante "screening" en la tira reactiva o membrana del cartucho, detectando selectivamente niveles elevados de drogas específicas en saliva.

[54] Los anticuerpos monoclonales tienen multitud de aplicaciones en la actualidad, tanto en investigación biomédica como en el diagnóstico y tratamiento de numerosas patologías. Esta cualidad de los anticuerpos monoclonales se debe a su alta especificidad y gran afinidad por la diana terapéutica.

Revista Científica del Centro Universitario de la Guardia Civil
Revista Lógos Guardia Civil

Artículo de Investigación

LA PROTECCIÓN DE LAS INFRAESTRUCTURAS CRÍTICAS SUBMARINAS Y EL FORTALECIMIENTO DE LA SEGURIDAD DEL MAR BÁLTICO: LA OPERACIÓN BALTIC SENTRY DE LA OTAN

Mónica Román González
Doctoranda en el Programa de Ciencias Políticas y de la Administración y Relaciones Internacionales de la Universidad Complutense de Madrid
Máster en Política Internacional: estudios sectoriales y de área en la Universidad Complutense de Madrid
monicaromangz@gmail.com
ORCID: https://orcid.org/0009-0007-8698-3739
Google Scholar: https://scholar.google.com/citations?user=2-KCa2kAAAAJ&hl=es&oi=sra

Recibido 31/03/2025
Aceptado 28/05/2025
Publicado 27/06/2025

Cita recomendada: Román, M. (2025). La protección de las infraestructuras críticas submarinas y el fortalecimiento de la seguridad del mar Báltico: La operación Baltic Sentry de la OTAN. *Revista Logos Guardia Civil*, 3(2), p.p. 221-256.

Licencia: Este artículo se publica bajo la licencia Creative Commons Atribución-NoComercial-SinDerivadas 4.0 Internacional (CC BY-NC-ND 4.0)
Depósito Legal: M-3619-2023
NIPO en línea: 126-23-019-8
ISSN en línea: 2952-394X

ORCID: https://orcid.org/0009-0007-8698-3739
Google Scholar: https://scholar.google.com/citations?user=2-KCa2kAAAAJ&hl=es&oi=sra

LA PROTECCIÓN DE LAS INFRAESTRUCTURAS CRÍTICAS SUBMARINAS Y EL FORTALECIMIENTO DE LA SEGURIDAD DEL MAR BÁLTICO: LA OPERACIÓN BALTIC SENTRY DE LA OTAN

Sumario: 1. INTRODUCCIÓN. 2. MARCO DEL ESTUDIO. 2.1. La importancia geoestratégica del Mar Báltico. 2.2. La protección de infraestructuras críticas submarinas. 2.3. La situación de las infraestructuras críticas submarinas en el Mar Báltico desde el inicio de la invasión rusa a gran escala de Ucrania en 2022. 3. LA OTAN Y LA PROTECCIÓN DE LAS INFRAESTRUCTURAS CRÍTICAS SUBMARINAS. 4. LA OPERACIÓN BALTIC SENTRY. 5. CONCLUSIONES Y PROPUESTAS. 6. REFERENCIAS BIBLIOGRÁFICAS.

Resumen: Los daños sobre los cables submarinos en el Mar Báltico han encendido las alarmas sobre una potencial guerra híbrida y la vulnerabilidad de las infraestructuras críticas submarinas occidentales ante posibles sabotajes, siendo así los reiterados incidentes sobre la zona señalada uno de los principales ejemplos de las tensiones geopolíticas existentes en la actualidad. El presente artículo tiene como principal objetivo analizar la Operación *Baltic Sentry* de la OTAN en un contexto en el que impera la creciente necesidad de la Alianza Atlántica de asegurar la protección de este tipo de infraestructuras críticas en el estratégico Mar Báltico y de reforzar así la seguridad sobre este último. Para ello, a través del empleo de métodos mixtos de investigación, el presente artículo primero explica la importancia de la protección de infraestructuras críticas submarinas en una zona de gran relevancia geoestratégica como es el mencionado Mar Báltico para después exponer el marco general de acción de la OTAN respecto a la protección de estas infraestructuras. Tras ello, el estudio expone las principales características de la Operación *Baltic Sentry* lanzada por la OTAN en enero de 2025 concluyendo que esta se ajusta a las necesidades requeridas para ser una buena estrategia capaz de permitir a la Alianza avanzar en la consecución de dos de sus principales objetivos prioritarios: la protección de unas infraestructuras cuya importancia es cada vez mayor como son las infraestructuras críticas submarinas y el consiguiente refuerzo de la seguridad en el Mar Báltico en pro de garantizar su resiliencia.

Abstract: Recent cases of undersea cable damage around the Baltic Sea have raised concerns about the possibility of a potential hybrid war and about the vulnerability of Western critical undersea infrastructure to possible acts of sabotage, with the repeated incidents over the area being one of the main examples of current geopolitical tensions. The aim of this article is to analyse NATO's Operation Baltic Sentry in a context in which the Atlantic Alliance needs to ensure the protection of this type of critical infrastructure in the Baltic Sea and thus to strengthen security over the latter. To this end, choosing mixed methods research design, this article explains the significance of the protection of critical undersea infrastructures in a region of tremendous geostrategic importance and then exposes the general framework of NATO's role in protecting these infrastructures. Therefore, the study sets out the main characteristics of Operation Baltic Sentry launched in January 2025, concluding that the analysed initiative meets the needs required for the efficient implementation of a strategy capable of enabling the Alliance to achieve two of its main security goals: the protection of undersea critical infrastructure and the strengthening of security in the Baltic Sea in order to reinforce its resilience.

ORCID: https://orcid.org/0009-0007-8698-3739
Google Scholar: https://scholar.google.com/citations?user=2-KCa2kAAAAJ&hl=es&oi=sra

Palabras clave: Organización del Tratado del Atlántico Norte (OTAN), Mar Báltico, infraestructuras críticas submarinas, seguridad, Baltic Sentry.

Keywords: North Atlantic Treaty Organization (NATO), Baltic Sea, Critical Undersea Infrastructure, security, Baltic Sentry.

ABREVIATURAS

CCD COE: *Cooperative Cyber Defence Centre of Excellence* o Centro de Excelencia Cooperativo de Ciberdefensa

CCOE: *Civil-Military Cooperation Centre of Excellence* o Centro de Excelencia de Cooperación Civil-Militar

CMRE: *Centre for Maritime Research and Experimentation* o Centro de Investigación y Experimentación Marítima de la OTAN

CONVEMAR: Convención de las Naciones Unidas sobre el Derecho del Mar

CRR: *Resilience Reference Curriculum* o Currículo de Referencia sobre Resiliencia

CTF: *Commander Task Force* o Comandante del Grupo de Trabajo

GNL: Gas Natural Licuado

GUGI: *Glavnoye upravlenie glubokovodnikh issledovanii* o Dirección Principal de Investigación de Aguas Profundas

MARCOM: *Allied Maritime Command* o Mando Naval de la OTAN en el Reino Unido

NATO: *North Atlantic Treaty Organization*

NSC: *NATO Shipping Centre*

OTAN: Organización del Tratado del Atlántico Norte

SOFCOM: *Allied Special Operations Forces Command* o Mando de las Fuerzas de Operaciones Especiales Aliadas

UE: Unión Europea

URSS: Unión de Repúblicas Socialistas Soviéticas

USV: *Unmanned Surface Vehicle* o Vehículo de superficie no tripulado

ZEE: Zona Económica Exclusiva

ORCID: https://orcid.org/0009-0007-8698-3739
Google Scholar: https://scholar.google.com/citations?user=2-KCa2kAAAAJ&hl=es&oi=sra

1. INTRODUCCIÓN

En los últimos tiempos, la importancia de las infraestructuras críticas submarinas ha aumentado drásticamente dado que estas facilitan la prestación de servicios básicos como la energía, las transacciones financieras, las comunicaciones o Internet. Esto convierte a la vulnerabilidad de estas infraestructuras en una preocupación de primer orden para los actores internacionales, especialmente teniendo en cuenta que el control de los fondos marinos continúa perfilándose como un elemento determinante en las relaciones de poder del presente siglo (Conte de los Ríos, 2025, p. 34). Y es que, si bien la reciente proliferación de la tecnología submarina y la consiguiente adquisición de la capacidad de realizar operaciones sofisticadas han favorecido sus capacidades de protección, semejantes innovaciones también ofrecen un abanico de posibilidades a aquellos actores que quieran aprovechar sus flaquezas (Cassetta, 2024, p. 2).

En este sentido, cualquier ataque contra la infraestructura submarina de la Organización del Atlántico Norte (OTAN) tendría serias consecuencias sobre la seguridad de sus Estados miembros, lo que le convierte en objetivo para sus rivales. Teniendo en cuenta que para realizar un ataque sobre estos cables se requiere de la disponibilidad de medios precisos, Rusia y en menor medida China son aquellos países que podrían identificarse como amenaza más directa según recoge el Insikt Group (2023, p. 11-15) en su último informe sobre los riesgos existentes para los cables submarinos.

Así, la denominada "guerra de los fondos marinos", más comúnmente conocida como *Seabed Warfare*, representa en la actualidad una amenaza inmediata para la Alianza Atlántica. Episodios como los repetidos incidentes sobre cables submarinos del geoestratégico Mar Báltico ponen de manifiesto la magnitud de los riesgos existentes ante una amenaza que requiere de una coordinación de esfuerzos e inversiones que ayuden a complementar las estrategias propias diseñadas por cada Estado. Es aquí donde entra en juego la importancia de la nueva operación de la OTAN en lo que se refiere a la protección de infraestructuras críticas submarinas en el Mar Báltico: la Operación *Baltic Sentry*.

Respecto a esta cuestión es variada la bibliografía a destacar. Por un lado, las principales razones que explican la importancia de proteger las infraestructuras críticas submarinas están ampliamente recogidas en investigaciones de expertos en la materia como Noelia Arjona Hernández (2023), Rafael García Pérez (2024) o Augusto Conte de los Ríos (2025). Por otro lado, respecto al papel de la OTAN en la protección de estas infraestructuras pueden destacarse el informe de Njall Trausti Fridbertsson (2023) o el artículo de Sean Monaghan, Otto Svendsen, Michael Darrah, y Ed Arnold para el *Center for Strategic & International Studies* (2023). Habida cuenta de ello, el presente estudio tiene como objetivo general analizar la recientemente anunciada Operación *Baltic Sentry* dentro del marco de actuación de la OTAN a la hora de reforzar la seguridad del Mar Báltico a través de la protección de sus infraestructuras críticas submarinas.

En consecuencia, la pregunta de investigación general que orienta el presente estudio es la siguiente: ¿Cómo responde la Operación *Baltic Sentry* de la OTAN a la protección de las infraestructuras críticas submarinas del Mar Báltico? La hipótesis general de la investigación sostiene que la Operación *Baltic Sentry* mejora la protección de las infraestructuras críticas submarinas del Mar Báltico y la presencia de la Alianza en el mismo, ajustándose así al nuevo contexto de amenazas existente.

Para ello, son dos los objetivos específicos delimitados. Primero, explicar la importancia de la protección de infraestructuras críticas submarinas en una zona de gran relevancia geoestratégica como es el mencionado Mar Báltico, especialmente ante el

actual contexto internacional marcado por la amenaza rusa tras su invasión a Ucrania y el aumento de daños sufridos por este tipo de infraestructuras desde entonces. Segundo, exponer el marco general de acción de la OTAN respecto a la protección de las infraestructuras críticas submarinas.

De esta manera, habiendo utilizado métodos mixtos de investigación, el estudio finaliza con la exposición de aquellas conclusiones respecto al nuevo proyecto de la OTAN en sus intentos por hacer frente a dos ejes cada vez más relevantes en materia de seguridad: la protección de infraestructuras críticas submarinas y el consiguiente fortalecimiento de la seguridad del Mar Báltico.

2. MARCO DEL ESTUDIO

2.1. LA IMPORTANCIA GEOESTRATÉGICA DEL MAR BÁLTICO

Ubicado en el norte de Europa (Ver Figura 1), el Mar Báltico ha sido históricamente un espacio de competencia geopolítica, que en la actualidad ha resurgido como un punto crucial de amenazas para la seguridad europea tras la invasión de Ucrania. Más allá de las prestaciones que ofrece a nivel comercial y de recursos marinos, este enclave constituye un centro clave para las infraestructuras que contribuyen significativamente al suministro de energía de varios Estados europeos, a su vez miembros de la OTAN (Fridbertsson, 2023, p. 2).

La propia Alianza lo define como "un centro vital para el comercio y el transporte energético que conecta a numerosas naciones aliadas" al ser un conducto tanto para el suministro de energía como un soporte a los cables submarinos que transfieren datos, dos elementos cruciales para la economía y seguridad de los aliados (NATO Allied Maritime Command, 2025a).

Figura 1

Mapa político del Mar Báltico.

Fuente: McNamara (2016).

ORCID: https://orcid.org/0009-0007-8698-3739
Google Scholar: https://scholar.google.com/citations?user=2-KCa2kAAAAJ&hl=es&oi=sra

Con la incorporación de Finlandia y Suecia a la OTAN en 2023 y 2024, el Mar Báltico ha pasado a ser denominado "el Lago de la OTAN". Sin embargo, esta etiqueta no es lo suficientemente adecuada teniendo en cuenta que los países aliados de la región se enfrentan aún a numerosas amenazas y, como define John Deni (2023), a un panorama dinámico de seguridad regional que les obliga a aunar esfuerzos a través de los diferentes marcos de cooperación de los que disponen. Esta situación se deriva principalmente de la presencia de Rusia sobre la zona, la cual plantea cada vez más desafíos a la seguridad de los aliados, especialmente en el contexto existente que convierte a la protección del denominado flanco oriental de la OTAN en una cuestión prioritaria para su seguridad.

Históricamente, Rusia ha sido uno de los principales jugadores de la región Báltica. Por un lado, cuenta con la ciudad portuaria de San Petersburgo, un importante centro económico y cultural del país por el que transita la mayor parte de su comercio marítimo desde tiempos de Pedro el Grande. Por otro, Rusia también controla el enclave de Kaliningrado situado entre Polonia y Lituania, donde cuenta con bases militares con la Flota del Báltico (Savitz y Winston, 2024, p. 5).

Además, actualmente en el Mar Báltico opera la denominada "Flota Fantasma rusa", una flota de petroleros creada por el Kremlin que navega bajo las banderas de otras naciones con el objetivo de evadir las sanciones impuestas tras su agresión ilegal a Ucrania (Childs, 2025, p 5). Al igual que otros buques rusos, esta está equipada con tecnología capaz de supervisar el lecho marino, por lo que es también sospechosa de participar en la campaña híbrida rusa contra Occidente a través de la recopilación de inteligencia y la consiguiente preparación de sabotajes sobre la infraestructura submarina crítica (Jones, 2025, p. 8). A ello hay que añadirle el hecho de que Moscú ha demostrado repetidamente sus ambiciones expansionistas sobre una región que podría ser su próximo objetivo, especialmente en su mayor momento de hostilidad hacia la OTAN.

En consecuencia, Rusia es el principal desafío para la Alianza en la región. En esta, Moscú encuentra las tácticas híbridas como principal herramienta para presionar a los aliados consiguiendo paliar sus debilidades militares convencionales y minimizar los riesgos de provocar un enfrentamiento directo entre las partes (Cassetta, 2024, p. 2). Como es conocido, los sabotajes se ejecutan de manera que resulta complejo identificar a los responsables, lo que provoca que los países afectados actúen con cautela al asignar responsabilidades por temor a escaladas. Así, resultan de utilidad a Rusia para mermar a la OTAN evitando la activación del artículo 5 de defensa colectiva (Jones, 2025, p. 3).

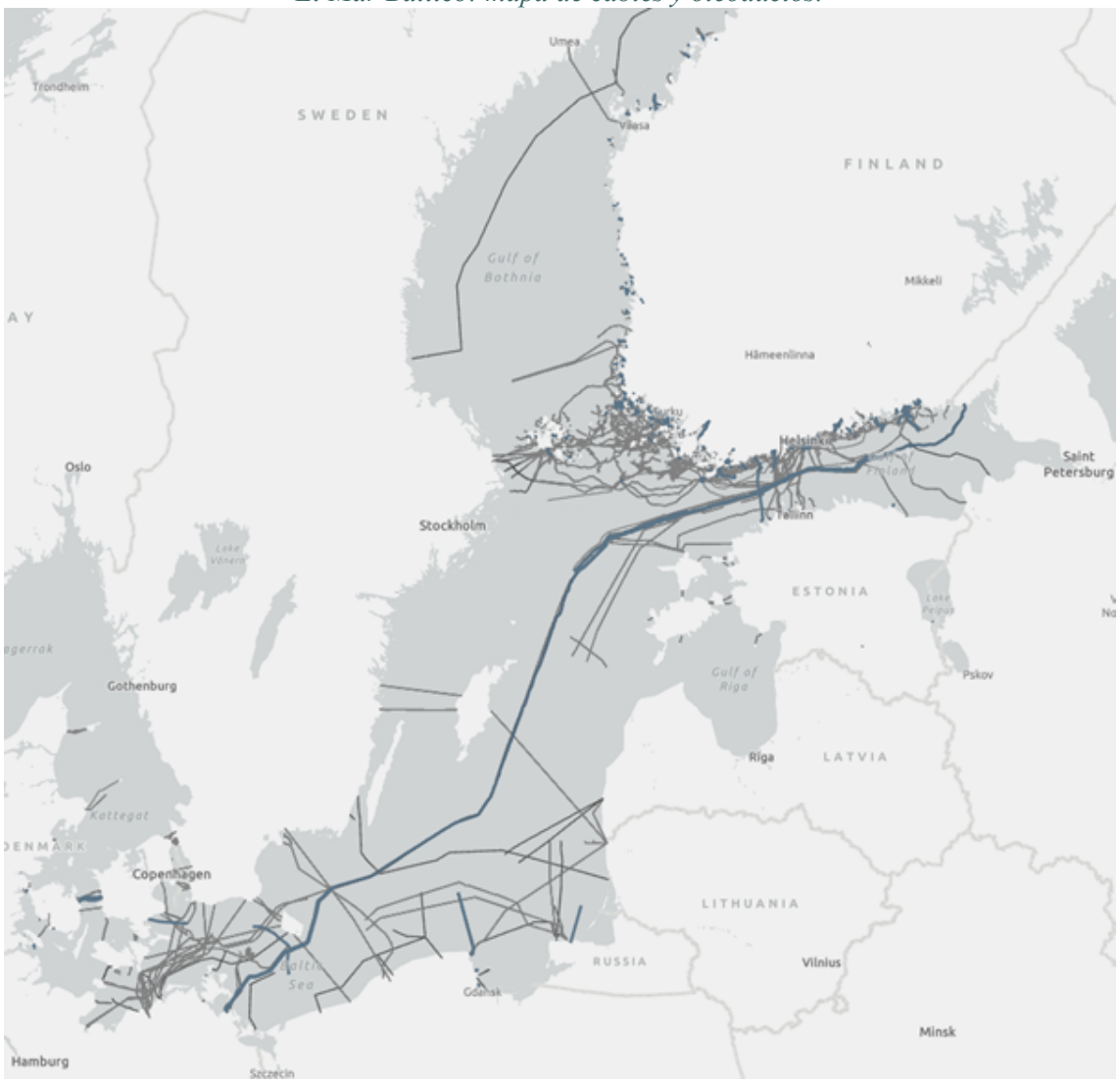
Paralelamente, cabe señalar que Rusia cuenta con unas capacidades submarinas que constituyen su principal fortaleza para competir en la región. Como explica Sidharth Kaushal (2023), Moscú cuenta con la Dirección Principal de Investigación de Aguas Profundas (*Glavnoye upravlenie glubokovodnikh issledovanii*, GUGI), una agencia secreta perteneciente al Ministerio de Defensa ruso que opera submarinos y buques capaces de participar en sabotajes.

Considerando que las capacidades rusas de ataque a infraestructuras críticas constituyen un componente fundamental de su estrategia (Fink y Kofman, 2020, p. 16), estas podrían ser empleadas para interceptar las comunicaciones esenciales en la región del Báltico (Metrick y Hicks, 2018, p. 7). Una región donde se encuentra una compleja

red de infraestructura submarina que resulta clave para la comunicación y la provisión energética entre las naciones europeas (Ver Figura 2).

Figura 2

El Mar Báltico: mapa de cables y oleoductos.



Fuente: Baltic Marine Environment Protection Commission (2024).

La protección de estas infraestructuras marítimas críticas en esta región geoestratégica clave depende en gran medida de la OTAN (Fridbertsson, 2023, p. 11), lo que abre una ventana de posibilidades a Moscú en su deseo de debilitar a Occidente.

2.2. LA PROTECCIÓN DE INFRAESTRUCTURAS CRÍTICAS SUBMARINAS

Las comunicaciones, transacciones financieras, energía y una gran diversidad de actividades diarias esenciales dependen de las infraestructuras críticas submarinas. Siguiendo los datos ofrecidos por el *Submarine Telecoms Forum* (2025, p. 8-9) en su último informe, el 99% del tráfico de datos internacionales transita a través de cables submarinos, lo que les convierte en "la columna vertebral de las comunicaciones mundiales".

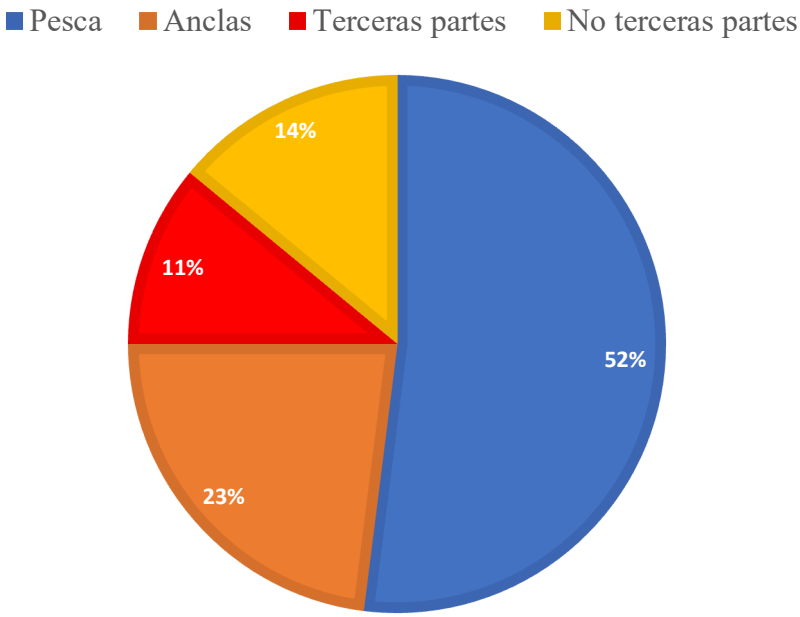
ORCID: https://orcid.org/0009-0007-8698-3739
Google Scholar: https://scholar.google.com/citations?user=2-KCa2kAAAAJ&hl=es&oi=sra

Su importancia es tal que cualquier daño sufrido puede suponer graves consecuencias sobre la estabilidad de la sociedad, lo que otorga a su seguridad una importancia geoestratégica clave siendo así un activo de valor incalculable cuya protección debe ser una prioridad en las agendas de seguridad (Quijarro Santibáñez, 2023, p. 15-22) (Fridbertsson, 2023, p. 2) (García Pérez, 2024, p. 265-298).

La creciente dependencia de las infraestructuras críticas submarinas junto a la actual convergencia de amenazas tradicionales y emergentes hacen que su protección sea uno de los mayores desafíos de seguridad (Conte de los Ríos, 2025, p. 26), especialmente atendiendo a su vulnerabilidad ante amenazas de origen natural o humano (Guilfoyle, Paige y McLaughlin, 2022, p. 657-696). El *International Cable Protection Committee* (2024, p. 5) sostiene que la interacción humana es la causa más común de daños en los cables, siendo estos generalmente causados por la pesca y las anclas (Ver Figura 3).

Figura 3

Gráfico de las principales causas de las interrupciones/roturas de cable según el International Cable Protection Committee.



Fuente: International Cable Protection Committee (2024, p. 5)

Ya en 2016, ante la creciente actividad de submarinos rusos hasta límites no conocidos desde la Guerra Fría, James Foggo y Alarik Fritz (2016) propusieron su idea de la existencia de "La Cuarta Batalla del Atlántico" en la que se verían amenazadas las infraestructuras submarinas, en concreto las plataformas de provisión energética y los cables de telecomunicaciones. Una batalla que, según el propio James Foggo (2023), empezó de manera evidente tras el aparente ataque al gasoducto Nord Stream en 2022.

Y es que, la señalada importancia de estas infraestructuras no sólo las ha convertido en un objetivo prioritario a proteger, sino también en un objetivo de posibles ataques para actores interesados en desestabilizar a otros. Incidentes como el mencionado han hecho que aumente la conciencia respecto a las vulnerabilidades que presentan estas infraestructuras en el marco de tensiones internacionales, lo que ha supuesto un punto de

inflexión a la hora de entender que la adopción de medidas para garantizar su protección es fundamental (Fridbertsson, 2023, p. 11) (Monaghan et al., 2023, p. 2).

Por otra parte, la constante evolución tecnológica conlleva importantes repercusiones en cuanto a las capacidades submarinas que los distintos actores deben adquirir (Clark, 2015, p. 18), algo que ha contribuido significativamente a la consolidación del ámbito submarino como el denominado "sexto dominio". Este nuevo dominio operacional, cada vez más disputado, concentra intereses económicos, estratégicos y militares debido a la riqueza de recursos que alberga y que le convierten en escenario de conflicto denominado *Seabed Warfare* (Conte de los Ríos, 2025, pp. 29–30). Aunque su conceptualización aún se encuentra en desarrollo por parte de actores como la OTAN, Conte de los Ríos (2025, p. 29) la define como el conjunto de operaciones realizadas en, hacia, desde, sobre y bajo el lecho marino con fines estratégicos o militares, utilizando el sabotaje del gasoducto Nord Stream como un caso representativo.

El ámbito marítimo es particularmente vulnerable a las amenazas híbridas. Además de que estas últimas son difíciles de distinguir de los daños accidentales, los agresores pueden utilizar la cobertura de buques de diversa índole que sean difíciles de rastrear, como por ejemplo buques pesqueros o privados (Monaghan et al., 2023, p. 6). En este sentido, cabe recordar que, al no ser considerado el sabotaje como una violación de la prohibición del uso de la fuerza según la Carta de Naciones Unidas, el derecho internacional restringe la respuesta militar ante los daños a cables, especialmente cuando están involucrados embarcaciones no militares (Conte de los Ríos, 2023, p. 33).

Christian Bueger y Tobias Liebetrau (2021) afirman que la gobernanza de las infraestructuras críticas submarinas tiene mayor complejidad debido a dos factores: (1) la necesidad de cooperación internacional por parte de diversos actores estatales -quienes actúan en base a sus beneficios estratégicos- y (2) el hecho de que parte de estas infraestructuras sean propiedad del sector privado -cuyo papel es relevante teniendo en cuenta que sus intereses pueden estar desalineados con los intereses de los Estados-. Esta complejidad dificulta la aplicación de disposiciones legales efectivas en caso de daños a las infraestructuras críticas submarinas (Conte de los Ríos, 2023, p. 32).

El régimen jurídico aplicable a la infraestructura submarina se sustenta en instrumentos internacionales, entre los cuales destacan la Convención para la Protección de los Cables de Telégrafos Submarinos de 1884 y la Convención de las Naciones Unidas sobre el Derecho del Mar (CONVEMAR) de 1982. Esta última establece que todos los Estados gozan del derecho a instalar cables y tuberías submarinos en la plataforma continental, conforme a la legislación nacional del Estado ribereño correspondiente (Arjona Hernández, 2023, p. 48). Asimismo, la CONVEMAR delimita diferentes espacios marítimos —aguas territoriales, Zonas Económicas Exclusivas (ZEE) y alta mar—, atribuyendo soberanía plena en las primeras, derechos limitados en las ZEE y un marco normativo menos definido en aguas internacionales, donde la actividad militar de otros Estados no puede ser legalmente restringida (McNamara, 2024).

Cabe señalar que entre los desafíos emergentes al derecho internacional marítimo se encuentran los vehículos submarinos no tripulados (Unmanned Underwater Vehicle, UUV) y los sistemas marítimos no tripulados (Unmanned Maritime Systems, MUS), cuyo estatus jurídico permanece indefinido. La ausencia de un marco normativo específico para su operación internacional complica su integración en los regímenes actuales, particularmente en lo referido a la CONVEMAR (Conte de los Ríos, 2023, p. 32). En este contexto, la creciente importancia de las infraestructuras críticas submarinas hace indispensable avanzar hacia un marco jurídico internacional efectivo que garantice su protección (García Pérez, 2023, p. 50).

ORCID: https://orcid.org/0009-0007-8698-3739
Google Scholar: https://scholar.google.com/citations?user=2-KCa2kAAAAJ&hl=es&oi=sra

Atendiendo a la importancia de estas infraestructuras y a su compleja legislación, Michael McNamara (2024) explica que, a medida que aumentan las tensiones geopolíticas entre Occidente y sus competidores, estas infraestructuras constituyen un objetivo al suponer las interferencias híbridas una herramienta útil en su propósito de desafiar los intereses de las democracias euroatlánticas. Estas enfrentan en la actualidad su principal amenaza en las acciones híbridas de Rusia (Monaghan et al., 2023, p. 2), particularmente en el Mar Báltico donde ha reforzado su presencia mediante la inversión en capacidades submarinas, consideradas su principal activo (Gresh, 2023, pp. 3-4).

Teniendo en cuenta el complejo contexto señalado y la situación del Mar Báltico, expertos como Conte de los Ríos (2025), Njall Trausti Fridbertsson (2023) y Monaghan et al (2023) coinciden en señalar una serie de elementos claves para definir una eficaz estrategia de protección. Reconociendo como fundamental reforzar las capacidades de detección, disuasión-prevención, adaptación y respuesta, los elementos a destacar son: (1) aumento de presencia o vigilancia, (2) colaboración entre actores, (3) coordinación con el sector privado, (4) tecnología avanzada, (5) marcos regulatorios, (6) medidas de respuesta y (7) renovar estrategias marítimas.

2.3. LA SITUACIÓN DE LAS INFRAESTRUCTURAS CRÍTICAS SUBMARINAS EN EL MAR BÁLTICO DESDE EL INICIO DE LA INVASIÓN RUSA A GRAN ESCALA DE UCRANIA EN 2022

El 26 de septiembre de 2022, la Autoridad Marítima Danesa informó de varias fugas de metano provocadas por una serie de explosiones submarinas frente a la isla danesa de Bornholm que dañaron seriamente el gasoducto Nord Stream (Ver Figura 4), consiguiendo cortar el suministro de gas ruso al mercado europeo a través de este (Energistyrelsen, 2022).

Figura 4

Mapa de los gasoductos Nord Stream 1 y Nord Stream 2 junto a las fugas de metano detectadas en septiembre de 2022.

Fuente: The European Space Agency (2022).

Independientemente de no conocerse quién fue el autor del aparente sabotaje, expertos coinciden en identificar este como punto de inflexión para los aliados a la hora de tomar en consideración aquellos esfuerzos necesarios para mejorar su capacidad de defenderse de posibles tácticas híbridas en el dominio submarino (Monaghan, 2022) (Fridbertsson, 2023) (Conte de los Ríos, 2025).

Un caso similar se registró en octubre de 2023 con el incidente ocurrido en el gasoducto Balticconnector. Esta infraestructura, junto con la terminal de gas natural licuado (GNL) Inkoo, salvaguarda la seguridad del suministro y la independencia energética de los países de la zona (Ver Figura 5).

Figura 5

Mapa de la red de transmisiones gasísticas en Finlandia y los Estados Bálticos.

Fuente: Gasgrid (s.f.)

ORCID: https://orcid.org/0009-0007-8698-3739
Google Scholar: https://scholar.google.com/citations?user=2-KCa2kAAAAJ&hl=es&oi=sra

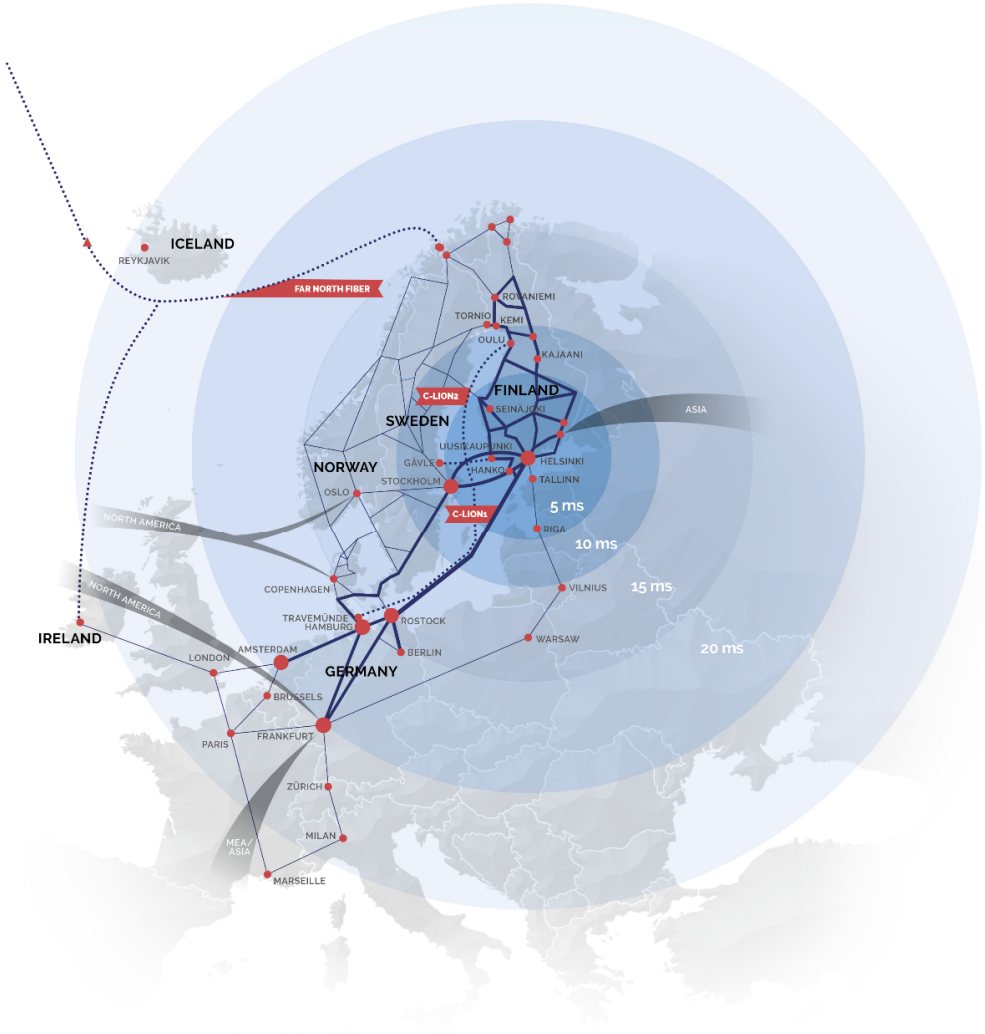
De acuerdo con los datos ofrecidos por la Oficina Nacional de Investigación de Finlandia, los daños al gasoducto fueron probablemente causados por el barco Newnew Polar Bear de una compañía naviera china que continuó su recorrido hacia aguas rusas escoltado por un rompehielos estatal del país euroasiático (Police of Finland, 2023a). Además, durante el incidente también fue detectado por la zona el Sevmorput, un carguero nuclear ruso (Police of Finland, 2023b).

La presunta participación de Rusia en este ataque podría estar orientada a desestabilizar el suministro energético de estos países, que dependían en gran medida del gas ruso hasta su prohibición como medida de respuesta a la invasión de Ucrania (Lietuvos Respublikos Energetikos Ministerija, 2022) (Latvijas Vēstnesis, 2022) (Republic of Estonia Ministry of Foreign Affairs, 2022) (Ministry of Economic Affairs and Employment of Finland, 2024). Ya en 2014, en los intentos de los Estados Bálticos por agilizar su desconexión del suministro ruso a través de la sincronización de sus redes eléctricas con el apoyo de la Unión Europea (UE), Lituania reportó casos de interferencia de buques militares rusos en la instalación del NordBalt, un cable de electricidad submarino que conecta al país con Suecia (McNamara, 2024).

En noviembre de 2024, el cable submarino C-Lion1, propiedad de la empresa finlandesa Cinia, fue dañado de manera aparentemente deliberada. Al ser este cable esencial para la comunicación directa entre Finlandia y Alemania (Ver Figura 6), estos daños provocaron la interrupción de las telecomunicaciones entre ambos Estados. Tal fue la gravedad del asunto que los Ministros de Asuntos Exteriores de estos países señalaron en una declaración conjunta que eran altas las sospechas de tratarse de un ataque intencionado, señalando que “la seguridad europea no sólo se ve amenazada por la guerra de agresión de Rusia contra Ucrania, sino también por la guerra híbrida de actores maliciosos” e instando a reforzar la defensa de este tipo de infraestructuras en la región (Ministry for Foreign Affairs of Finland, 2024).

Figura 6

Mapa de la conectividad entre los Estados Nórdicos y Europa Central a través de los cables submarinos C-Lion1 y C-Lion2.



Fuente: Cinia (s.f.)

De manera simultánea, el cable de telecomunicaciones BCS East-West Interlink que conecta Lituania y Suecia resultó dañado como consecuencia de "algo más que un accidente", tal y como señaló Andrius Šemeškevičius, Jefe de Tecnología de la compañía Telia Lietuva, a la cadena nacional lituana LRT TV (2024).

Las investigaciones emprendidas por los países afectados por ambos incidentes se centraron en el buque chino Yi Peng 3, el cual había zarpado previamente del puerto ruso Ust-Luga. Ante la imposibilidad de abordar el buque, las fuerzas navales danesas vigilaron de cerca su situación una vez entró en el estrecho de Kattegat, según confirmaron en sus redes sociales (Forsvaret, 2024). Atendiendo a las declaraciones de Šemeškevičius a LRT TV (2024), las probabilidades de tratarse de un sabotaje son bastante altas puesto que los cables de ambos incidentes se cruzan (Ver Figura 7).

ORCID: https://orcid.org/0009-0007-8698-3739
Google Scholar: https://scholar.google.com/citations?user=2-KCa2kAAAAJ&hl=es&oi=sra

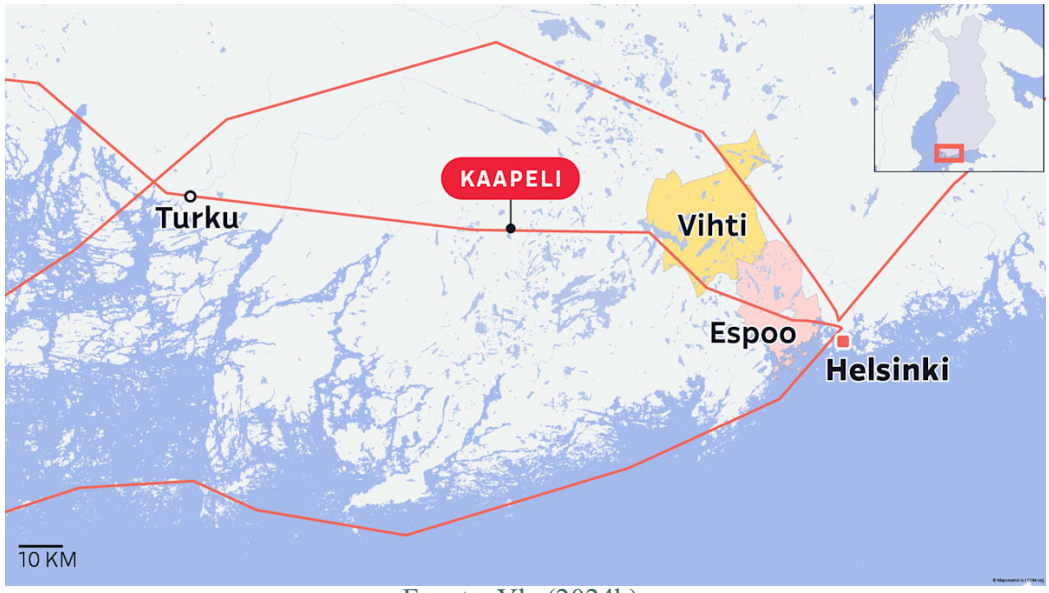
Figura 7
Mapa de los cables submarinos dañados en el Mar Báltico en noviembre de 2024 y la ubicación del buque Yi Peng 3.

Fuente: Reuters (2024).

Un mes después, el 3 de diciembre de 2024, la empresa finlandesa GlobalConnect informó que sus cables de telecomunicaciones que conectan al país con Suecia habían sufrido daños en dos puntos diferenciados entre las zonas de Vithi y Espoo (Ver Figura 8), tal y como confirmó el gerente de comunicaciones de la empresa, Niklas Ekström, a la cadena pública finlandesa Yle (2024a). Sin embargo, la policía del país señaló en un comunicado que no había indicios de tratarse de un sabotaje, sino más bien de un accidente por daños causados durante unas excavaciones (Police of Finland, 2025a).

Figura 8

Mapa del cable submarino de la empresa finlandesa GlobalConnect dañado en diciembre de 2024.

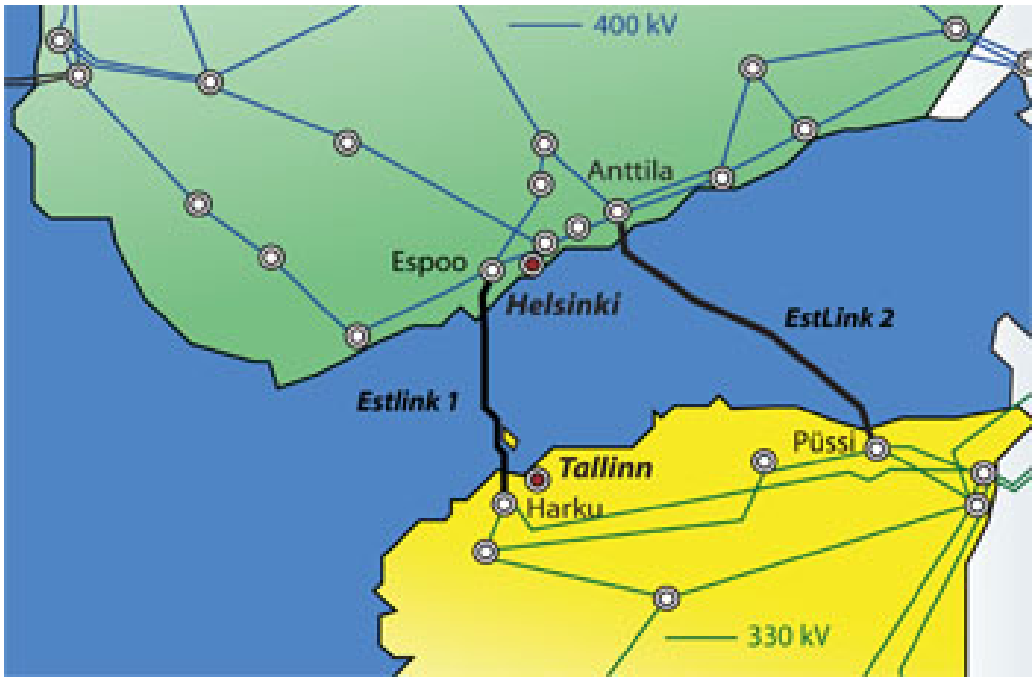


Fuente: Yle (2024b).

El 25 de diciembre de 2024, la operadora finlandesa Fingrid informó que fue dañado el cable submarino Estlink 2 de la red eléctrica que conecta Finlandia y Estonia (Ver Figura 9). Finlandia inició una investigación por sabotaje e incautó el petrolero Eagle S de la "Flota Fantasma rusa", ya que este se encontraba en la zona transportando petróleo ruso causando aparentemente los daños al arrastrar su ancla (Police of Finland, 2025b). Este suceso hizo que la OTAN anunciase a finales de diciembre su intención de reforzar su presencia militar en el Mar Báltico para prevenir futuros incidentes y abordar posibles nuevas amenazas a estas infraestructuras (NATO, 2024a).

Figura 9

Mapa de la conectividad entre Finlandia y Estonia a través de los cables submarinos Estlink 1 y Estlink 2.



Fuente: Fingrid (s.f.).

ORCID: https://orcid.org/0009-0007-8698-3739
Google Scholar: https://scholar.google.com/citations?user=2-KCa2kAAAAJ&hl=es&oi=sra

El 26 de enero de 2025 se descubrieron daños en un cable de comunicaciones entre Suecia y Letonia (Ver Figura 10) según informó la empresa responsable Latvia State Radio and Television Center (2025). Si bien el país nórdico inició una investigación preliminar por sabotaje e incautó al carguero búlgaro Vezhen, finalmente la fiscalía sueca determinó que la rotura del cable entre ambos países no fue consecuencia de un ataque deliberado sino de un accidente (Swedish Prosecution Authority, 2025). De igual forma, a petición de las autoridades letonas ante sus sospechas respecto al mismo incidente, Noruega incautó el buque Silver Dania cuya tripulación era rusa y el cual navegaba entre San Petersburgo y Múrmansk (Politiet, 2025).

Figura 10

Mapa del cable submarino en el Mar Báltico que conecta Letonia y Suecia dañado en enero de 2025.

Fuente: Reuters (2025).

En febrero de 2025 otro cable submarino que conecta Finlandia y Alemania sufrió daños en la ZEE de Suecia, concretamente cerca de la isla sueca de Gotland. Si bien Finlandia ha iniciado ya una investigación sobre los daños sufridos por el cable que pertenece a una de sus empresas (Police of Finland, 2025c), desde Suecia se habla de un posible sabotaje. Patrik Johansson, jefe del Departamento de Agua y Saneamiento de la región afectada de Gotland, confirmó tras la primera revisión del lugar que la principal causa fue la influencia humana (Region Gotland, 2025).

Simultáneamente, la empresa finlandesa Cinia (2025) volvió a informar de perturbaciones en el funcionamiento del cable submarino C-Lion1. A pesar de que la investigación sigue en marcha, el medio alemán Kieler Nachrichten (2025) informó que las autoridades germanas investigaron al carguero Arne, un barco sospechoso de formar

parte de la "Flota Fantasma rusa" que navegaba por la zona bajo la bandera de Antigua y Barbuda y que se dirigía de San Petersburgo a Sevilla sin una de sus anclas, lo que incrementa las sospechas de un aparente sabotaje orquestado por el Kremlin.

Estos incidentes demuestran que las infraestructuras críticas submarinas de la zona son vulnerables a posibles ataques. Ya en 2017, el Comandante de la fuerza submarina de la OTAN, Andrew Lennon, confirmó la existencia de "actividad submarina rusa en la proximidad de cables submarinos" a unos niveles hasta ahora no conocidos, lo que pone de manifiesto el interés estratégico de Rusia en la infraestructura submarina de la OTAN (Birnbaum, 2017). Como señalan Monaghan et al. (2023, p. 1), estos posibles ataques están "destinados a perturbar la cohesión transatlántica y la actividad económica, socavar el apoyo occidental a Ucrania y dar forma a posibles operaciones militares futuras". Por ello, la situación desde el inicio de la guerra a gran ha hecho que la seguridad en este ámbito sea una prioridad para la OTAN.

3. LA OTAN Y LA PROTECCIÓN DE LAS INFRAESTRUCTURAS CRÍTICAS SUBMARINAS

A nivel general, la protección de las infraestructuras críticas submarinas para la OTAN se enmarca en varios artículos de su tratado constitutivo. Concretamente en el artículo 2 sobre colaboración económica, el artículo 3 sobre resiliencia y el artículo 5 sobre la defensa colectiva recogidos en el Tratado del Atlántico Norte (1949). Respecto a este último, el Nuevo Concepto Estratégico de la OTAN (2022) menciona las amenazas híbridas contra infraestructuras críticas, reafirmando su inclusión en el marco del artículo citado y destacando el compromiso con la cooperación internacional para su protección.

La creciente preocupación por la protección de estas infraestructuras ha convertido a su seguridad en un objetivo de especial relevancia para la OTAN. Teniendo en cuenta su importancia para el funcionamiento de la sociedad, amenazas como el control adquirido por empresas chinas sobre algunas de estas infraestructuras y la creciente actividad rusa cerca de las mismas hicieron que en 2020 la Alianza Atlántica considerase el estado de su infraestructura crítica (García Pérez, 2023, p. 3).

Respecto a esto último, el entonces Secretario General de la OTAN, Jens Stoltenberg (2020) resaltó la importancia de la infraestructura submarina crítica dentro de los esfuerzos de la Alianza para reforzar su resiliencia:

> I think it's important to address this, because it is important to understand that most of these cables are privately owned and it's publicly known where they are. And that makes them potentially vulnerable. So we need to monitor the potential vulnerabilities. That's partly the reason why we have produced this report. We have tools to protect them and to monitor threats. And we have also established a new Atlantic Command in Norfolk, a new NATO command in Norfolk. And one of the tasks of this new North Atlantic Command is also to look into how to protect, how to monitor threats against undersea infrastructure. For instance, the internet is dependent on these cables and that just highlights the importance of the undersea cables. One of the main issues at the meeting today was resilience, and that's about civilian infrastructure, health services, telecommunications. But, of course, as part of our effort to strengthen the resilience, undersea cables, undersea infrastructure is an important part of that.

ORCID: https://orcid.org/0009-0007-8698-3739
Google Scholar: https://scholar.google.com/citations?user=2-KCa2kAAAAJ&hl=es&oi=sra

Sin embargo, la adopción de las principales medidas orientadas a la protección de estas infraestructuras se dio tras el inicio de la guerra a gran escala en Ucrania en 2022. Hasta entonces, esta cuestión se integraba dentro de la labor de limitadas instituciones ligadas en su mayoría al ámbito marítimo o a contrarrestar las amenazas híbridas, siendo especialmente reseñables dos de ellas.

Por un lado, el *Strengthened Resilience Commitment*, creado en 2021 por decisión de los Jefes de Estado y de Gobierno de la OTAN en el que se reconoce el compromiso de la Alianza para intensificar los esfuerzos para garantizar la resiliencia de sus infraestructuras críticas (NATO, 2021). Por otro lado, el *NATO Resilience Committe,* un organismo responsable de la dirección político-estratégica, la orientación, la planificación y la coordinación general de las actividades de resiliencia en la Alianza Atlántica (NATO, 2022) (Ver Tabla 1).

Tabla 1

Instituciones de la OTAN en las que se enmarcaba la protección de infraestructuras críticas antes de la guerra a gran escala de Ucrania de 2022.

	Instituciones destacadas
2006	*NATO Shipping Centre (NSC)*
2007	*Civil-Military Cooperation Centre of Excellence (CCOE)*
2008	*Cooperative Cyber Defence Centre of Excellence (CCD COE)*
2012	*NATO Allied Maritime Command (MARCOM)*
	Multinational Maritime Security Centre of Excellence (MARSEC COE)
2014	*Strategic Communications Centre of Excellence*
2018	*Counter Hybrid Support Teams*
2021	*Strengthened Resilience Commitment*
2022	*NATO Resilience Committe*

Fuente: Elaboración propia a partir de lo ofrecido por la OTAN en sus sitios web

Como respuesta al aparente sabotaje del Nord Stream de finales de 2022, la OTAN creó en febrero de 2023 la *Critical Undersea Infrastructure Coordination Cell* (NATO, 2023a). Un mes antes de la adopción de esta medida, el 11 de enero de 2023, se anunció la creación de un grupo de trabajo OTAN-UE sobre la resiliencia de las infraestructuras críticas en el marco del actual Diálogo Estructurado OTAN-UE sobre Resiliencia, dentro del cual se encuentra integrado (European Commission & NATO, 2023, p. 2).

En su informe publicado en el mes de junio de 2023, ambas partes señalan la existencia de una diversidad de amenazas a las que hay que enfrentar, las cuales abarcan desde posibles ataques terroristas hasta desastres naturales. No obstante, señalan de manera directa que desde la agresión rusa a Ucrania estas infraestructuras se han convertido en un activo vulnerable cuya protección debe ser prioritaria (European Commission & NATO, 2023, p. 4).

Otro ejemplo de los efectos del incidente en el Nord Stream como punto de inflexión para reforzar los esfuerzos occidentales sobre la resiliencia de sus infraestructuras críticas submarinas es la creación del *NATO Maritime Centre for the Security of Critical Undersea Infrastructure* (NMCSCUI) en la Cumbre de Vilna de 2023:

> The threat to critical undersea infrastructure is real and it is developing. We are committed to identifying and mitigating strategic vulnerabilities and dependencies with respect to our critical infrastructure, and to prepare for, deter and defend against the coercive use of energy and other hybrid tactics by state and non-state actors. Any deliberate attack against Allies' critical infrastructure will be met with a united and determined response; this applies also to critical undersea infrastructure. The protection of critical undersea infrastructure on Allies' territory remains a national responsibility, as well as a collective commitment. NATO stands ready to support Allies if and when requested. We have agreed to establish NATO's Maritime Centre for the Security of Critical Undersea Infrastructure within NATO's Maritime Command (MARCOM). We also agreed to set up a network that brings together NATO, Allies, private sector, and other relevant actors to improve information sharing and exchange best practice (NATO, 2023b)

En consonancia con lo expresado por Stoltenberg (2020) y con el informe conjunto de la Comisión Europea y la OTAN (2023, p. 3), el Comunicado de la Cumbre de Vilna reafirma la creciente preocupación de la Alianza por las amenazas dirigidas contra las infraestructuras críticas submarinas. En el señalado extracto, la OTAN reconoce la necesidad de identificar proactivamente sus vulnerabilidades, subraya que dichas amenazas pueden emanar tanto de actores estatales como no estatales y destaca la importancia de una coordinación efectiva con actores relevantes, especialmente del sector privado. Asimismo, se contempla explícitamente la posibilidad de que ataques híbridos contra estas infraestructuras puedan ser considerados como actos que justifiquen la activación del artículo 5 de defensa colectiva del Tratado del Atlántico Norte.

Por ello, en mayo de 2024 el NMCSCUI fue inaugurado. La OTAN define este como un centro de redes y conocimiento especializado en infraestructuras submarinas críticas, cuya función principal es apoyar los procesos de toma de decisiones estratégicas, facilitar el despliegue operativo de fuerzas y coordinar acciones conjuntas para garantizar su protección. Todo ello se articula mediante la integración de esfuerzos entre los Estados miembros, socios estratégicos y el sector privado (NATO Media Centre, 2024).

No obstante, esta no es la única medida resultante de la Cumbre de Vilna implementada por la OTAN en aras de garantizar un mejor abordaje de las amenazas en el ámbito señalado. En octubre de 2023 se aprobó la *Digital Ocean Vision*, una iniciativa destinada a mejorar la comprensión del dominio marítimo mediante una mayor armonización de las capacidades nacionales y aliadas dedicadas a la vigilancia marítima haciendo uso de una diversa gama de activos (NATO, 2023c).

Por otra parte, ante los crecientes desafíos a estas infraestructuras, el 23 de mayo de 2024 la OTAN celebró la primera reunión de la Red de Infraestructuras Submarinas Críticas por decisión de los Ministros de Defensa con el fin de mejorar la coordinación y el intercambio de información. En el encuentro se discutieron medidas como el refuerzo de patrullas navales, el fomento de la innovación tecnológica y el uso de capacidades avanzadas de detección y respuesta, consolidando el papel central de la Alianza en este ámbito (NATO, 2024b).

En noviembre de 2024 se llevó a cabo el Ejercicio *Bold Machina 24* en La Spezia, Italia, coordinado por el *Allied Special Operations Forces Command* (SOFCOM) y el

ORCID: https://orcid.org/0009-0007-8698-3739
Google Scholar: https://scholar.google.com/citations?user=2-KCa2kAAAAJ&hl=es&oi=sra

Centre for Maritime Research and Experimentation (CMRE) con el objetivo de probar sensores submarinos orientados a la protección de infraestructuras críticas (NATO Centre for Maritime Research and Experimentation, 2024, p. 2). Este tipo de ejercicios refleja el mencionado interés en integrar tecnologías emergentes, como sistemas no tripulados, para reforzar la seguridad en el dominio submarino (Conte de los Ríos, 2025, p. 26).

En este sentido, es también reseñable que la OTAN ha desarrollado nuevas herramientas que permitan a los aliados detectar cualquier actividad sospechosa para protegerse de posibles sabotajes. Estas incluyen el uso de la inteligencia artificial como demuestra el caso de *Mainsail,* una herramienta de software desarrollada por el CMRE que detecta los buques que se comportan de forma sospechosa con la intención de recopilar información sobre la infraestructura submarina y de dañar esta última (NATO Multimedia, 2025).

Respecto a la protección específica de la infraestructura submarina del Mar Báltico, la OTAN ha promovido la innovación tecnológica necesaria para una eficaz detección de cualquier actividad sospechosa que complemente el trabajo de sus patrullas en la región. Unas medidas progresivamente intensificadas como consecuencia directa del aparente sabotaje al Nord Stream, tal y como reconoce la propia Alianza (NATO, 2023d).

En febrero de 2025, con el propósito de avanzar en su integración operativa en tareas de vigilancia marítima en el Mar Báltico, la OTAN llevó a cabo una demostración de vehículos de superficie no tripulados (Unmanned Surface Vehicle, USV) en la región. Esta iniciativa se enmarca en los esfuerzos de la Alianza por incorporar tecnologías emergentes y disruptivas -como los sistemas autónomos y la inteligencia artificial- orientadas a optimizar la conciencia situacional y a fortalecer la protección de las infraestructuras submarinas críticas, en particular a lo largo de las líneas marítimas de comunicación (NATO Allied Maritime Command, 2025b). Además, en el marco del Comité de Resiliencia, la OTAN presentó en 2025 su primer *Resilience Reference Curriculum* con el objetivo de fortalecer la capacidad aliada frente a amenazas, incluidas las dirigidas a infraestructuras críticas (NATO, 2025a).

Paralelamente, la cooperación con la Unión Europea ha cobrado relevancia a través de iniciativas como el *EU Hybrid Toolbox*, la *Hybrid Fusion Cell* y los *Hybrid Rapid Response Teams*, concebidas para fomentar sinergias y reforzar la coordinación anti-híbrida con la OTAN (European External Action Service, 2022, p. 34). Esta convergencia en las iniciativas entre las entidades señaladas demuestra la importancia de desarrollar sólidas capacidades defensivas, por lo que su coordinada implementación junto a la efectiva integración de nuevas tecnologías y capacidades operativas resultan fundamentales para garantizar una exitosa protección de las infraestructuras submarinas europeas, especialmente teniendo en cuenta la rápida evolución de las amenazas que afectan a este ámbito (Conte de los Ríos, 2025, p. 33).

Finalmente, cabe señalar que la OTAN plantea el fortalecimiento de la cooperación con el sector privado como una dimensión clave para mejorar su capacidad de respuesta frente a las amenazas dirigidas a infraestructuras críticas submarinas. Esta cooperación se justifica, por una parte, por el hecho de que una proporción significativa de dichas infraestructuras es de propiedad o gestión privada, y por otra, por el potencial

del sector privado para aportar soluciones tecnológicas esenciales ante un entorno operativo cada vez más complejo (Fridbertsson, 2023, p. 11).

4. LA OPERACIÓN BALTIC SENTRY

El 14 de enero de 2025, la OTAN celebró una Cumbre de Aliados del Mar Báltico en la que se abordaron las crecientes amenazas a la infraestructura submarina crítica de la región. Como resultado, el Secretario General de la Alianza Atlántica y los participantes publicaron la *Joint Statement of the Baltic Sea NATO Allies Summit* (2025) con la que se anunciaba el lanzamiento de una iniciativa militar orientada a reforzar la protección de estas infraestructuras: la Operación *Baltic Sentry*.

Alegando una profunda preocupación por el incremento de acciones que amenazan el funcionamiento de infraestructuras críticas submarinas, la Alianza señaló su disposición a "disuadir, detectar y contrarrestar cualquier intento de sabotaje" y a responder a cualquier ataque "con una respuesta firme y decidida" (Tasavallan Presidentti, 2025). Todo ello en un momento en el que la OTAN reconoce la necesidad de modernizar sus capacidades para fortalecer su disuasión y defensa en aras de abordar y contrarrestar las cambiantes amenazas a la seguridad (Tasavallan Presidentti, 2025).

El MARCOM, bajo la dirección del Mando Conjunto de Fuerzas Brunssum (*Joint Forces Command Brunssum*, JFCBS), reconoce desempeñar un papel fundamental en la coordinación de las operaciones dentro de lo que define como una "actividad de vigilancia multidominio cuyo objetivo es aumentar el conocimiento de la situación marítima en el Mar Báltico para disuadir y defenderse de ataques a las infraestructuras críticas submarinas" (NATO Allied Maritime Command, 2025a). Con ese objetivo, la Operación *Baltic Sentry* incluye el despliegue de activos adicionales en el mar, aire y tierra por parte de los aliados que permitan mejorar la vigilancia y la disuasión.

Realizando patrullas regulares y ejercicios conjuntos, la OTAN busca mantener una presencia constante en el Mar Báltico que se vea monitoreada continuamente por buques de guerra, submarinos, aeronaves y el apoyo de tecnología avanzada de vigilancia marítima. Por ejemplo, los barcos del *Standing NATO Maritime Group 1* (SNMG1) y del *Standing NATO Mine Countermeasures Group 1* (SNMCMG1) participarán en *Baltic Sentry* junto con otras embarcaciones de patrulla marítima aliadas, al mismo tiempo que la OTAN continuará invirtiendo en el marco de esta operación en tecnología militar de vanguardia destinada a detectar y minimizar amenazas como es el caso de la inteligencia artificial, sensores avanzados o sistemas de sonar especializados (MARCOM, 2025).

A ello se le suma la inclusión de dos actores clave en el seno de la Alianza. Por un lado, la recientemente inaugurada *Commander Task Force* (CTF) en el propio Mar Báltico con sede en la ciudad portuaria de Rostock. Esta, además de encargarse de la coordinación de los buques aliados en el Báltico, trabaja para lograr la construcción de una visión regional unificada respecto a la infraestructura crítica en el Mar Báltico, con el propósito de apoyar los esfuerzos de la OTAN en cuanto a su protección estratégica (Tasavallan Presidentti, 2025). Por otro, el ya mencionado NMCSCUI centrará sus esfuerzos en proteger y asegurar los activos submarinos vitales (Tasavallan Presidentti, 2025).

Para alcanzar tales objetivos, la OTAN considera fundamental no sólo trabajar en el marco de la propia Alianza, sino colaborar y cooperar con otros actores que van desde

ORCID: https://orcid.org/0009-0007-8698-3739
Google Scholar: https://scholar.google.com/citations?user=2-KCa2kAAAAJ&hl=es&oi=sra

la UE hasta el sector privado. Mientras en el primer caso la cooperación se centrará en reforzar los mecanismos ya existentes, en el caso del sector privado la OTAN destaca la relevancia de cooperar con los operadores de infraestructuras y las empresas de tecnología de vanguardia a la hora de elaborar las diferentes medidas de respuesta necesarias para aumentar la resiliencia (Tasavallan Presidentti, 2025).

La Alianza Atlántica prevé asimismo la adopción de nuevas medidas conforme al derecho internacional, orientadas tanto a la prevención como a la respuesta ante amenazas o actos irresponsables contra infraestructuras críticas submarinas en la región (Tasavallan Presidentti, 2025). En el marco del lanzamiento de la Operación *Baltic Sentry*, el actual Secretario General de la OTAN, Mark Rutte, subrayó la necesidad de una aplicación estricta del marco jurídico vigente, advirtiendo que cualquier potencial amenaza contra estas infraestructuras podría acarrear medidas coercitivas como el abordaje, la incautación o la detención de embarcaciones. En este contexto, señaló la respuesta de Finlandia ante los incidentes como un ejemplo destacado de actuación (NATO, 2025b).

La puesta en marcha de estas medidas se justifica en la constante mención de la existencia de amenazas. Respecto a estas últimas se menciona una amenaza en concreto, la denominada “Flota Fantasma rusa”. Esta es definida como una amenaza significativa para la seguridad marítima y medioambiental tanto en la región del Mar Báltico como a nivel global, ya que compromete la integridad de la infraestructura submarina, incrementa los riesgos asociados a las municiones químicas arrojadas en el fondo marino y representa una fuente importante de financiación para la guerra de agresión ilegal de Rusia contra Ucrania (Tasavallan Presidentti, 2025).

De la misma forma, se reconoce que la amenaza hacia las infraestructuras submarinas críticas no se limita al Mar Báltico. Por ello, se señala que la operación *Baltic Sentry* supone asimismo un punto de inflexión para favorecer a una mayor cooperación para fortalecer la resiliencia de estas infraestructuras críticas y, por ende, fortalecer la seguridad de la OTAN. De ahí que la puesta en marcha de la propia operación vaya de la mano con el anuncio de la renovación de la estrategia marítima de la alianza (Tasavallan Presidentti, 2025).

5. CONCLUSIONES Y PROPUESTAS

Las infraestructuras críticas submarinas son vitales para la economía y el sistema mundial de comunicaciones. Su creciente relevancia y los constantes avances tecnológicos en esta cuestión han hecho que estas se conviertan en un objetivo prioritario de defensa, pero también de posibles ataques. De esta manera, lo que se conoce como *Seabed Warfare* ha dejado de ser un concepto lejano para pasar a convertirse en una amenaza inmediata para los Aliados. El estrecho vínculo entre la seguridad de estas infraestructuras y la estabilidad global, principalmente en términos económicos y de comunicaciones, hacen que su protección y la gestión de sus vulnerabilidades sea actualmente una prioridad en términos de defensa para cualquier actor internacional.

Atendiendo al contexto actual de rivalidad con una Rusia que anuncia públicamente sus deseos de desestabilizar a la OTAN, esto convierte hoy en día a la implementación de estrategias de protección de las infraestructuras críticas en un objetivo de extrema urgencia para la defensa de la Alianza Atlántica, especialmente sobre la región

Báltica. Como se ha mencionado en el documento, el Mar Báltico no sólo constituye por sus prestaciones un enclave de competencia geopolítica entre la OTAN y Rusia, sino también una zona clave para la seguridad de las infraestructuras críticas submarinas que garantizan la estabilidad de los aliados. Por ello, aunar esfuerzos sobre esta región en lo que se refiere a reforzar su seguridad debe ser una prioridad para la OTAN, especialmente desde la guerra de Ucrania de 2022 y la adhesión de Suecia y Finlandia a la Alianza.

Esto permite ofrecer la principal conclusión ligada al objetivo específico número uno del presente estudio. Si bien la protección de estas infraestructuras debe ser ya de por sí un objetivo para la OTAN teniendo en cuenta su importancia para la resiliencia de la sociedad y su extrema vulnerabilidad ante un gran abanico de amenazas, actualmente la situación geopolítica convierte a estas infraestructuras en un claro objetivo de posibles ataques. Esto se demuestra con el aumento de incidentes en los cables submarinos en el Mar Báltico desde el inicio del conflicto en 2022, habiendo ocurrido hasta la fecha ocho incidentes en los que infraestructuras críticas de la región han quedado dañadas, ocurriendo prácticamente la totalidad de ellos dentro de la ZEE de Finlandia y Suecia, países que casualmente solicitaron desde ese mismo año entrar en la OTAN a pesar de la férrea oposición del Kremlin (Ver Tabla 2).

Tabla 2

Incidentes en la infraestructura crítica submarina del Mar Báltico desde 2022.

	Infraestructura	**Lugar del incidente**	**Países afectados**	**Causas**
Nord Stream	Gasoducto submarino	ZEE de Suecia y Dinamarca	Unión Europea	Altos indicios de sabotaje
Balticconnector	Gasoducto submarino	ZEE de Finlandia	Finlandia y Estonia	Altos indicios de sabotaje
C-Lion 1	Cable de telecomunicaciones	ZEE de Suecia	Finlandia y Alemania	Altos indicios de sabotaje
BCS East-West Interlink	Cable de Telecomunicaciones	ZEE de Suecia	Lituania y Suecia	Altos indicios de sabotaje
GlobalConnect	Cables de telecomunicaciones	ZEE de Finlandia	Finlandia y Suecia	Accidente
Estlink 2	Red eléctrica	ZEE de Suecia	Finlandia y Estonia	Altos indicios de sabotaje
Latvia State Radio and Television Center	Cable de telecomunicaciones	ZEE de Suecia	Suecia y Letonia	Accidente
Gotland	Cable marítimo propiedad de una empresa finlandesa	ZEE de Suecia	Finlandia y Alemania	Altos indicios de sabotaje

Fuente: Elaboración propia

ORCID: https://orcid.org/0009-0007-8698-3739
Google Scholar: https://scholar.google.com/citations?user=2-KCa2kAAAAJ&hl=es&oi=sra

En relación con el segundo objetivo específico del presente estudio sobre el marco general de acción de la OTAN respecto a la protección de las infraestructuras críticas submarinas, son varias las conclusiones a destacar. A pesar del desgaste del Ejército ruso en su desempeño en la guerra de Ucrania y los duros reveses sufridos en el ámbito naval, las tácticas híbridas rusas siguen siendo la amenaza más apremiante para la infraestructura europea en el Mar Báltico. La OTAN se posiciona como actor central en la prevención de ataques contra estas infraestructuras, intensificando sus esfuerzos con la progresiva adopción de medidas desde 2022 tras la invasión de Ucrania y los posteriores incidentes.

Mientras que esta cuestión se integraba dentro de la labor de instituciones ligadas en su mayoría al ámbito marítimo, desde el aparente sabotaje al Nord Stream -en pleno contexto de tensiones con Moscú- la OTAN ha adoptado casi una decena de medidas. Pueden destacarse la creación de la *Critical Undersea Infrastructure Coordination Cell* o la *NATO Maritime Centre for the Security of Critical Undersea Infrastructure*, la iniciativa *Digital Ocean Vision,* la realización de ejercicios militares como *Bold Machina 24*, la innovación tecnológica necesaria para aprovechar la inteligencia artificial como *Mainsail* o la adopción de iniciativas complementarias con terceros actores como la UE.

La Operación *Baltic Sentry* constituye la principal respuesta de la OTAN al desafío que supone la protección de infraestructuras críticas submarinas en el Mar Báltico y reforzar la seguridad de la región. Cumpliendo con el objetivo principal del estudio centrado en el análisis de esta Operación, puede observarse que las medidas implantadas en su marco se orientan al fortalecimiento de las capacidades de detección, disuasión-prevención, adaptación y respuesta, estando así en línea con los principales criterios propuestos por la literatura especializada para adoptar una estrategia eficaz (Ver Tabla 3).

Tabla 3

Aplicación de los elementos necesarios para una estrategia efectiva de protección de la infraestructura crítica submarina en el marco de la Operación Baltic Sentry de la OTAN.

	Operación Baltic Sentry de la OTAN
Aumento de presencia o vigilancia	✓
Colaboración con actores internacionales	✓
Coordinación con el sector privado	✓
Uso de tecnología avanzada	✓
Desarrollo de marcos regulatorios	✓
Renovación de la estrategia marítima	✓
Implementación de medidas de respuesta	✓

Fuente: Elaboración propia a partir de Conte de los Ríos (2025), Monaghan et al. (2023), Fridbertsson (2023) y la información proporcionada por la OTAN

En definitiva, la Operación *Baltic Sentry* demuestra que las infraestructuras submarinas críticas son actualmente identificadas por la OTAN como una vulnerabilidad estratégica cuya protección es esencial para garantizar la resiliencia y la seguridad no sólo de la Alianza, sino para el día a día de la sociedad. Una lección que encuentra en los diferentes episodios ocurridos en el marco de la guerra de Ucrania desde 2022 un punto

de inflexión, siendo destacable el aparente ataque al Nord Stream a finales del mismo año tal y como demuestran tanto el marco cronológico de las medidas adoptadas por la OTAN en este sector como lo expuesto por la propia Alianza a la hora de justificar estas últimas.

De esta manera, respondiendo a la pregunta general del estudio, se cumple la hipótesis general de la investigación sostiene que la Operación *Baltic Sentry* mejora la protección de las infraestructuras críticas submarinas del Mar Báltico y la presencia de la Alianza en el mismo, ajustándose así al nuevo contexto de amenazas existente.

REFERENCIAS BIBLIOGRÁFICAS

Arjona Hernández, N. (2023). La protección de los cables submarinos de telecomunicaciones: Soberanías digitales y seguridad de la red de cable submarina. *Revista Internacional De Pensamiento Político*, *18*(18), pp. 41–67. https://doi.org/10.46661/revintpensampolit.8753

Baltic Marine Environment Protection Commission. (2024). *HELCOM Map and Data Service.* https://maps.helcom.fi/website/mapservice/

Baltic Marine Environment Protection Commission. (2024). *HELCOM Map and Data Service*. https://maps.helcom.fi/website/mapservice/

Birnbaum, M. (22 de diciembre de 2017). Russian submarines are prowling around vital undersea cables. It's making NATO nervous. *The Washington Post.* https://www.washingtonpost.com/world/europe/russian-submarines-are-prowling-around-vital-undersea-cables-its-making-nato-nervous/2017/12/22/d4c1f3da-e5d0-11e7-927a-e72eac1e73b6_story.html?hpid=hp_hp-top-table-main_russiasubs712pm%3Ahomepage%2Fstory

Bueger, C., Liebetrau, T., y Franken, J. (2022). *Security Threats to Undersea Communications Cables and Infrastructure - Consequences for the EU*. European Parliament In-Depth Analysis, https://www.europarl.europa.eu/RegData/etudes/IDAN/2022/702557/EXPO_IDA(2022)702557_EN.pdf

Bueger, C., y Liebetrau, T. (2021). Protecting hidden infrastructure: The security politics of the global submarine data cable network. *Contemporary Security Policy*, *42*(3), pp. 391–413. https://doi.org/10.1080/13523260.2021.1907129

Cassetta, M. (2024). How to Respond to the Emerging Threats to Critical Underwater Infrastructure at the Time of Russia's War Against Ukraine. *Istituto Affari Internazionali (IAI), IAI Commentaries 24-31 June 2024*, pp. 1-5. https://www.iai.it/en/pubblicazioni/c05/how-respond-emerging-threats-critical-underwater-infrastructure

Childs, N. (2025). Russia's 'Shadow Fleet' and Sanctions Evasion: What Is To Be Done?. *The International Institute for Strategic Studies (IISS), January 2025*, pp. 1-15. https://www.iiss.org/globalassets/media-library---content--migration/files/research-papers/2025/01/russias_shadow-fleet_and-sanctions-evasion/iiss_russias_shadow-fleet_and-sanctions-evasion_31012025.pdf

Cinia. (20 de febrero de 2025). *Disturbance in Cinia's C-Lion Submarine Cable*. https://www.cinia.fi/en/news/disturbance-in-cinia-c-lion-submarine-cable

Cinia. (s.f.). *International connectivity by Cinia.* https://www.cinia.fi/hubfs/Cinia%20Theme%202024/Muut%20kuvat/Cinian-kansainvaliset-verkkoyhteydet-kartta.jpg

Clark, B. (2015). *The Emerging Era in Undersea Warfare*. Center for Strategic and Bidgetary Assessments (CSBA), https://csbaonline.org/research/publications/undersea-warfare

Conte de los Ríos, A. (2025). Amenazas a la seguridad: los fondos marinos y las infraestructuras críticas. *Global Affairs Journal*, (7), pp. 26-35. https://www.unav.edu/documents/16800098/147587031/amenazas-seguridad.pdf

Deni, J. R. (18 de diciembre de 2023). *Is the Baltic Sea a NATO Lake?*. Carnegie Endowment for International Peace. https://carnegieendowment.org/research/2023/12/is-the-baltic-sea-a-nato-lake?lang=en

Energistyrelsen. (26 de septiembre de 2022). *Leak at North Stream 2 in the Baltic Sea*. https://ens.dk/en/press/leak-north-stream-2-baltic-sea

European Commission & NATO. (2023). *EU-NATO TASK OF FORCE ON THE RESILIENCE OF CRITICAL INFRASTRUCTURE. FINAL ASSESMENT REPORT.* https://www.nato.int/cps/en/natohq/news_216631.htm

European External Action Service. (2022). *A STRATEGIC COMPASS FOR SECURITY AND DEFENCE: For a European Union that protects its citizens, values and interests and contributes to international peace and security.* https://www.eeas.europa.eu/sites/default/files/documents/strategic_compass_en3_web.pdf

Fingrid. (s.f.). *EstLink 2 – second high-voltage direct current link between Finland and Estonia*. https://www.fingrid.fi/en/grid/construction/arkisto/estlink-2/

Fink, A. y Kofman, M. (2020). Russian Strategy for Escalation Management: Key Debates and Players in Military Thought. *CNA Information Memorandum, April 2020*, pp. 1-48. https://www.cna.org/cna_files/pdf/DIM-2020-U-026101-Final.pdf

Foggo, J. (17 de enero de 2023). The Fourth Battle of the Atlantic Is Underway. *Center for European Policy Analysis (CEPA),* https://cepa.org/article/the-fourth-battle-of-the-atlantic-is-underway/

Foggo, J. y Fritz, A. (2016). The Fourth Battle of the Atlantic. *U.S. Naval Institute, 142*(6), https://www.usni.org/magazines/proceedings/2016/june/fourth-battle-atlantic

Forsvaret. [@forsvaretdk]. (20 de noviembre de 2024). *Regarding the Chinese ship Yi Peng 3: The Danish Defence can confirm that we are present in the area near the Chinese ship Yi Peng 3. The Danish Defence currently has no further comments.* [Post en X]. X. https://x.com/forsvaretdk/status/1859195509866381402

Fridbertsson, N. T. (2023). *Protecting Critical Maritime Infrastructure – The Role of Technology.* General Report. 032 STC 23 E. NATO Parliamentary Assembly: Science and Technology Committee (STC). https://www.nato-

pa.int/document/2023-critical-maritime-infrastructure-report-fridbertsson-032-stc

García Pérez, R. (2023). España en la red global de cables submarinos. *Instituto Español de Estudios Estratégicos, Documento Marco IEEE 10/2023*, pp. 1-51. https://www.defensa.gob.es/ceseden/-/espa%C3%B1a-en-la-red-global-de-cables-submarinos

García Pérez, R. (2024). "La seguridad de los cables submarinos", en Fernándo Ibáñez Gómez (Coord.), *Seguridad marítima. Una incertidumbre permanente*, Bosch Editor, Barcelona, pp. 265-298.

Gasgrid. (s.f.). *Map of Finnish and Baltic gas transmissions*. https://gasgrid.fi/wp-content/uploads/Gasgrid_maakaasu_lisaversiot_eu_EN-scaled.jpg

Gasum. (2023). *Gasum has terminated its pipeline natural gas supply contract with Gazprom Export.* https://www.gasum.com/en/news-and-customer-stories/news-and-press-releases/2023/gasum-has-terminated-its-pipeline-natural-gas-supply-contract-with-gazprom-export/#:~:text=The%20parties%20were%20not%20able,details%20of%20the%20contract%20termination.

Gresh, G. F. (2023). *Europe's new maritime security reality: Chinese ports, Russian bases, and the rise of subsea warfare*. Foreign Policy at Brookings, Policy Brief, February 2023. https://www.brookings.edu/articles/europes-new-maritime-security-reality-chinese-ports-russian-bases-and-the-rise-of-subsea-warfare/

Guilfoyle, D., Paige, T. P., y McLaughlin, R. (2022). THE FINAL FRONTIER OF CYBERSPACE: THE SEABED BEYOND NATIONAL JURISDICTION AND THE PROTECTION OF SUBMARINE CABLES. *International and Comparative Law Quarterly*, *71*(3), pp. 657–696. https://doi.org/10.1017/S0020589322000227

Insikt Group. (2023). *The Escalating Global Risk Environment for Submarine Cables*. Recorded Future Threat Analysis, https://www.recordedfuture.com/research/escalating-global-risk-environment-submarine-cables

International Cable Protection Committee. (2024). *Report of the International Cable Protection Committee Docs: HSSC16-07.10A: ICPC activities affecting HSSC.* International Hydrographic Organization, Tokyo, Japan, 27-31 May 2024. https://iho.int/uploads/user/Services%20and%20Standards/HSSC/HSSC16/HSSC16_2024_07.10A_EN_ICPC%20activities%20affecting%20HSSC.pdf

Jones, S. G. (2025). Russia's Shadow War Against the West. *Center for Strategic and International Studies (CSIS), CSIS Briefs March 2025*, pp. 1-20. https://www.csis.org/analysis/russias-shadow-war-against-west

Kaushal, S. (25 de mayo de 2023). *Stalking the Seabed: How Russia Targets Critical Undersea Infrastructure*. Royal United Services Institute (RUSI), May 2023. https://www.rusi.org/explore-our-research/publications/commentary/stalking-seabed-how-russia-targets-critical-undersea-infrastructure

Kieler Nachrichten. (2025). *Verdacht der Sabotage: Ermittler suchen Anker vom russischen Frachter „Arne“* [Sospecha de sabotaje: Investigadores buscan el ancla del carguero ruso "Arne"]. https://www.kn-online.de/schleswig-holstein/verdacht-der-sabotage-gegen-russischen-frachter-arne-in-kiel-ermittlungsstand-ORSQRUDZZRGJHC7KSCB4SKJCDM.html

Latvia State Radio and Television Center. (2025). *LVRTC Submarine Optical Fiber Cable Damaged.* https://www.lvrtc.lv/en/news/jaunumi/lvrtc-submarine-optical-fiber-cable-damaged/

Latvijas Vēstnesis. (28 de julio de 2022). *Grozījumi Enerģētikas likumā* [Reformas a la Ley de Energía]. https://www.vestnesis.lv/op/2022/144.5

Lietuvos Respublikos Energetikos Ministerija. (20 de mayo de 2022). *No more Russian oil, gas and electricity imports in Lithuania from Sunday*. https://enmin.lrv.lt/en/news/no-more-russian-oil-gas-and-electricity-imports-in-lithuania-from-sunday/

LRT TV. (18 de noviembre de 2024). *Undersea cable between Lithuania and Sweden damaged – Telia.* https://www.lrt.lt/en/news-in-english/19/2416006/undersea-cable-between-lithuania-and-sweden-damaged-telia?srsltid=AfmBOoowPquC_SbY0w-dUT2dfxJTzPrj-OPvif6IxXoDTJQuKnQx11fF

McNamara, E. M. (17 de marzo de 2016). *Securing the Nordic-Baltic region*. NATO Review. https://www.nato.int/docu/review/articles/2016/03/17/securing-the-nordic-baltic-region/index.html

McNamara, E. M. (28 de agosto de 2024). Reforzar la resiliencia: el papel de la OTAN en la mejora de la seguridad de las infraestructuras submarinas críticas. *NATO Review: Opinion, Analysis and debate on Security Issues*, https://www.nato.int/docu/review/articles/2024/08/28/reinforcing-resilience-natos-role-in-enhanced-security-for-critical-undersea-infrastructure/index.html

Ministry for Foreign Affairs of Finland. (18 de noviembre de 2024*). Joint statement by the Foreign Ministers of Finland and Germany on the severed undersea cable in the Baltic Sea.* https://um.fi/statements/-/asset_publisher/6zHpMjnolHgl/content/joint-statement-by-the-foreign-ministers-of-finland-and-germany-on-the-severed-undersea-cable-in-the-baltic-sea/35732

Ministry of Economic Affairs and Employment of Finland. (7 de mayo de 2024). *Hallituksen esitys laiksi maakaasun ja nesteytetyn maakaasun maahantuonnin väliaikaisesta kieltämisestä Venäjän federaatiosta ja Valko-Venäjältä* [La propuesta del gobierno de ley sobre la prohibición temporal de la importación de

gas natural y gas natural licuado de la Federación de Rusia y Bielorrusia]. https://tem.fi/en/project?tunnus=TEM036:00/2024

Monaghan, S. (6 de octubre de 2022). Five Steps NATO Should Take after the Nord Stream Pipeline Attack. *Center for Strategic and International Studies (CSIS)*, https://www.csis.org/analysis/five-steps-nato-should-take-after-nord-stream-pipeline-attack

NATO Allied Maritime Command. (2025a, 14 de enero de 2025). *NATO's Baltic Sentry steps up patrols in the Baltic Sea to safeguard Critical Undersea Infrastructure.* https://mc.nato.int/media-centre/news/2025/nato-baltic-sentry-steps-up-patrols-in-the-baltic-sea-to-safeguard-critical-undersea-infrastructure

NATO Allied Maritime Command. (2025b, 20 de febrero de 2025). *NATO Conducts Unmanned Surface Vehicle Demonstration in Baltic Sea.* https://mc.nato.int/media-centre/news/2025/page228602539

NATO Centre for Maritime Research and Experimentation. (2024). *NATO STO CMRE NEWSLETTER*. January-June 2024. https://www.cmre.nato.int/wp-content/uploads/2024/09/v2%20NATO%20STO%20CMRE%20Newsletter_1_20240712_114854_0000_EDITED_4PAGES%20(002).pdf

NATO Media Centre. (2024, 28 de mayo de 2024). *NATO officially launches new Maritime Centre for Security of Critical Undersea Infrastructure.* https://mc.nato.int/media-centre/news/2024/nato-officially-launches-new-nmcscui

NATO Multimedia. (06 de febrero de 2025). *Protecting undersea cables with artificial intelligence.* https://www.natomultimedia.tv/app/asset/718197

NATO. (2021, 14 de junio de 2021). *Strengthened Resilience Commitment*. https://www.nato.int/cps/en/natohq/official_texts_185340.htm

NATO. (2022, 07 de octubre de 2022). *Resilience Committee*. https://www.nato.int/cps/in/natohq/topics_50093.htm

NATO. (2023a, 15 de febrero de 2023). *NATO stands up undersea infrastructure coordination cell*. https://www.nato.int/cps/en/natohq/news_211919.htm

NATO. (2023b, 11 de julio de 2023). *Vilnius Summit Communiqué. Issued by NATO Heads of State and Government participating in the meeting of the North Atlantic Council in Vilnius 11 July 2023.* https://www.nato.int/cps/en/natohq/official_texts_217320.htm

NATO. (2023c, 12 de octubre de 2023). *NATO Defence Ministers launch initiative to enhance maritime surveillance capabilities*. https://www.nato.int/cps/ra/natohq/news_219441.htm

NATO. (2023d, 19 de octubre de 2023). *NATO steps up Baltic Sea patrols after subsea infrastructure damage.* https://www.nato.int/cps/en/natohq/news_219500.htm

NATO. (2024a, 30 de diciembre de 2024). *NATO to enhance military presence in the Baltic Sea*. https://www.nato.int/cps/en/natohq/news_231800.htm

NATO. (2024b, 23 de mayo de 2024). *NATO holds first meeting of Critical Undersea Infrastructure Network.* https://www.nato.int/cps/en/natohq/news_225582.htm

NATO. (2025a, 21 de febrero de 2025). *NATO launches the Resilience Reference Curriculum.* https://www.nato.int/cps/en/natohq/news_233458.htm

NATO. (2025b, 14 de enero de 2025). *NATO launches 'Baltic Sentry' to increase critical infrastructure security*. https://www.nato.int/cps/en/natohq/news_232122.htm

Police of Finland. (2025b, 2 de marzo de 2025). *Eagle S tanker to move to international waters under Border Guard's control.* https://poliisi.fi/en/-/eagle-s-tanker-to-move-to-international-waters-under-border-guard-s-control

Police of Finland. (2023a, 24 de octubre de 2023). *National Bureau of Investigation has clarified technically the cause of gas pipeline damage*. https://poliisi.fi/en/-/national-bureau-of-investigation-has-clarified-technically-the-cause-of-gas-pipeline-damage

Police of Finland. (2023b, 17 de octubre de 2023). *National Bureau of Investigation examines background of vessels sailing in the gas pipeline damage area*. https://poliisi.fi/en/-/national-bureau-of-investigation-examines-background-of-vessels-sailing-in-the-gas-pipeline-damage-area

Police of Finland. (2025a, 3 de diciembre de 2025). *Police do not suspect any criminal offence in either of the cable damage incidents in Southern Finland.* https://poliisi.fi/en/-/police-do-not-suspect-any-criminal-offence-in-either-of-the-cable-damage-incidents-in-southern-finland

Police of Finland. (2025c, 21 de febrero de 2025). *National Bureau of Investigation to conduct a preliminary inquiry into suspected cable damage in Baltic Sea.* https://poliisi.fi/en/-/national-bureau-of-investigation-to-conduct-a-preliminary-inquiry-into-suspected-cable-damage-in-baltic-sea

Politiet. (31 de enero de 2025). *Ship can leave Tromsø*. https://www.politiet.no/aktuelt-tall-og-fakta/aktuelt/nyheter/2025/01/31/troms2/

Quijarro Santibáñez, L. (2023). Seabed Warfare: La guerra submarina del Siglo XXI. *Revista de Marina, 141*(997), pp. *15-22.* https://revistamarina.cl/revista/997

Region Gotland. (3 de marzo de 2025). *Misstänkt sabotage* [Sospecha de sabotaje]. https://gotland.se/bygga-bo-och-miljo/vatten-och-avlopp/dricksvatten/misstankt-sabotage

ORCID: https://orcid.org/0009-0007-8698-3739
Google Scholar: https://scholar.google.com/citations?user=2-KCa2kAAAAJ&hl=es&oi=sra

Republic of Estonia Ministry of Foreign Affairs. (2022). *Estonia imposes a ban on natural gas imports and purchases from Russia.* https://www.vm.ee/en/news/estonia-imposes-ban-natural-gas-imports-and-purchases-russia

Reuters. (2024). *Damaged fibre-optic cables in the Baltic Sea*. https://www.reuters.com/graphics/BALTICSEA-CABLES/zdpxqaaxwvx/chart.png

Reuters. (2025). *Damaged fibre-optic cable in the Baltic Sea*. https://www.reuters.com/graphics/BALTIC-SECURITY/xmvjbdamavr/chart.png

Stoltenberg, J. (22 de octubre de 2020). *Online press conference by NATO Secretary General Jens Stoltenberg following the first day of the meetings of NATO Defence Ministers.* https://www.nato.int/cps/en/natohq/opinions_178946.htm?selectedLocale=en

Submarine Telecoms Forum. (2025). *Global Outlook.* SubTel Forum Magazine #140. https://subtelforum.com/subtel-forum-magazine-140-global-outlook/

Swedish Prosecution Authority. (2025). *Prosecutor revokes decision on seized ship.* https://www.aklagare.se/en/media/press-releases/2025/february/prosecutor-revokes-decision-on-seized-ship/?_t_id=ajCngOfkVK4qcLdxSmm4EA%3d%3d&_t_uuid=ajbjBKKES7uVHPgMJkVsvA&_t_q=baltic&_t_tags=language%3aen%2csiteid%3a764c28f6-3ce5-48e7-a8ec-b8f5f22e4245%2candquerymatch&_t_hit.id=Aklagare_Web_Business_PressReleases_Models_PressReleasePage/_847c0fdb-df1d-4d16-9b4a-0db494be3af4_en&_t_hit.pos=2

Tasavallan Presidentti. (14 de enero de 2025). *Joint Statement of the Baltic Sea NATO Allies Summit*. https://www.presidentti.fi/joint-statement-of-the-baltic-sea-nato-allies-summit/

The European Space Agency. (06 de octubre de 2022). *Nordstream pipeline map with shipping traffic.* https://www.esa.int/ESA_Multimedia/Images/2022/10/Nordstream_pipeline_map_with_shipping_traffic

Yle. (2024a, 31 de diciembre de 2024). *Police: No crime suspected in Finland-Sweden cable break.* https://yle.fi/a/74-20128835

Yle. (2024b). *The cable was damaged in two separate places between Espoo and Vihti. Image: Laura Merikalla / Yle, Mapcreator, OpenStreetMap, GlobalConnect*. https://images.cdn.yle.fi/image/upload/c_crop,h_1080,w_1919,x_0,y_0/ar_1.7777777777777777,c_fill,g_faces,h_675,w_1200/dpr_2.0/q_auto:eco/f_auto/fl_lossy/v1733216443/39-1389673674ec7f18a492

NORMATIVA

Convención de las Naciones Unidas sobre el Derecho del Mar, Nueva York, 30 de abril de 1982. https://www.un.org/depts/los/convention_agreements/texts/unclos/convemar_es.pdf

Convención para la Protección de los Cables de Telégrafos Submarinos, París, 14 de marzo de 1884. https://iscpc.org/information/Convention_on_Protection%20_of_Cables_1884.pdf

Nuevo Concepto Estratégico de la OTAN, Madrid, 29 de junio de 2022. https://www.defensa.gob.es/Galerias/main/nuevo_concepto_estrat_gico_de_la_otan.pdf

Tratado del Atlántico Norte, Washington, 4 de abril de 1949. https://www.nato.int/cps/en/natohq/official_texts_17120.htm?selectedLocale=es

ORCID: https://orcid.org/0009-0007-8698-3739
Google Scholar: https://scholar.google.com/citations?user=2-KCa2kAAAAJ&hl=es&oi=sra

Revista Científica del Centro Universitario de la Guardia Civil

Revista Lógos Guardia Civil

Artículo de Investigación

EL CAPITAL INTELECTUAL EN LA INSTITUCIÓN DE LA GUARDIA CIVIL Y SU CONTRIBUCIÓN A LA ECONOMÍA SOCIAL

Virginia Belén Subiris Moriel
Doctoranda en la Universidad Rey Juan Carlos.
Programa Ciencias Sociales y Jurídicas. Rama Empresarial
Master International Human Resources Management
(Dirección Internacional de Recursos Humanos)
virbelsu@gmail.com
ORCID: Https://orcid.org/0009-0000-2569-3710

Recibido 31/03/2025
Aceptado 10/06/2025
Publicado 27/06/2025

Cita recomendada: Subiris, V. (2025). El capital intelectual en la institución de la Guardia Civil y su contribución a la economía social. *Revista Logos Guardia Civil*, 3(2), p.p. 257-292.

Licencia: Este artículo se publica bajo la licencia Creative Commons Atribución-NoComercial-SinDerivadas 4.0 Internacional (CC BY-NC-ND 4.0)
Depósito Legal: M-3619-2023
NIPO en línea: 126-23-019-8
ISSN en línea: 2952-394X

ORCID: Https://orcid.org/0009-0000-2569-3710

EL CAPITAL INTELECTUAL EN LA GUARDIA CIVILY SU CONTRIBUCIÓN A LA ECONOMÍA SOCIAL

Sumario: 1. INTRODUCCIÓN. 2. MARCO TEÓRICO. 2.1. Capital Intelectual. 2.2. Economía Social y el Cuerpo de la Guardia Civil. 3. METODOLOGÍA. 4. RESULTADOS Y DISCUSIÓN. 5. CONCLUSIONES Y PROPUESTAS. 6. REFERENCIAS BIBLIOGRÁFICAS.

Resumen: La seguridad es un tema clave para la cooperación entre los países que conforman la Unión Europea en el entorno socioeconómico actual. Esto implica que las políticas del sector público no sólo fortalezcan las capacidades en defensa, sino que también implementen medidas que contribuyan a la seguridad económica y social. Conectando estos términos: seguridad, cooperación, público y economía social, nos lleva a pensar en una institución que los ha alineado en su estrategia, durante más de 181 años de existencia, la Institución de la Guardia Civil. Sin embargo, no se han encontrado investigación, artículos o proyectos que aborden esta cuestión en el ámbito académico. El presente estudio analiza cómo el capital intelectual (CI) de la institución, contribuye a generar valor económico-social a través de sus acciones solidarias y humanitarias. La metodología utilizada se basa en un análisis de contenido de la información divulgada de su CI en sus memorias de responsabilidad social y de sostenibilidad entre 2014-2023. Se ha empleado el modelo Intellectus adaptado al contexto público, para identificar y cuantificar los activos intangibles. Los resultados evidencian que el CI de la Institución, a través de la gestión del conocimiento, la cultura organizativa, las relaciones externas, el carácter benemérito y el compromiso social aporta valor tangible e intangible que va más allá de sus funciones de seguridad pública. Esta investigación demuestra la relevancia del CI en instituciones públicas y su potencial en el fortalecimiento de una economía social integrada en la Agenda 2030.

Abstract: Security is a key issue for cooperation among the countries that make up the European Union in the current socioeconomic environment. This implies that public sector not only strengthen defense capabilities but also implement measures that contribute to economic and social security. Conecting these terms—security, cooperation, public, and social economy— leads us to an institution that has aligned them in its strategy for more than 181 years of existence: the Civil Guard. However, no research, articles, or projects addressing this issue have been found in the academic field. This study analyzes how the institution's intellectual capital (IC) contributes to generating economic and social value through its solidarity and humanitarian actions. The methodology used is based on a content analysis of the information disclosed by its IC in its social responsibility and sustainability reports between 2014 and 2023. The Intellectus model, adapted to the public context, is used to identify and quantify intangible assets. The results show that the institution's IC, through knowledge management, organizational culture, external relations, worthy character, and social commitment, provides tangible and intangible value that goes beyond its public safety functions. This research demonstrates the relevance of IC in public institutions and its potential to strengthen the social economy integrated into the 2030 Agenda.

Palabras clave: economía social, capital intelectual, guardia civil, sostenibilidad, valor social.

Keywords: social economy, intellectual capital, civil guard, sustenability, social value.

ORCID: Https://orcid.org/0009-0000-2569-3710

ABREVIATURAS

ASGC: Asociación de Guardias Civiles Solidarios.

CEPES: Confederación Empresarial Española de la Economía Social.

CE: Capital Estructural.

CH: Capital Humano.

CI: Capital Intelectual.

CIC: Centro de Investigación sobre la Sociedad del Conocimiento.

CIS: Centro de Investigación Sociológica.

CR: Capital Relacional.

EUROPOL: Policía Europea.

IADE: Instituto de Administración de Empresas.

KBW: Knowledge- Based View.

MITES: Ministerio de Trabajo y Economía Social.

MRSCGC: Memoria de Responsabilidad Social Corporativa de la Guardia Civil.

MS: Memoria de Sostenibilidad.

RBV: Resources- Based View.

RSC: Responsabilidad Social Corporativa.

ODS: Objetivos de Desarrollo Sostenible.

OECC: Oficina Española del Cambio Climático

OECD: Organisation for Economic Co-operation and Development.

ONG: Organización no gubernamental.

ONU: Organización de las Naciones Unidas.

OTAN: Organización del Atlántico Norte.

UE: Unión Europea.

VRIN: Valor, Rareza, Inimitabilidad y No Sustituibilidad.

1. INTRODUCCIÓN

La economía social, es un modelo económico focalizado en el interés colectivo que pone a las personas en el centro de su actividad priorizando tanto la cooperación como la sostenibilidad y la solidaridad antes que el lucro individual (Retolaza & Alzola, 2021). El desarrollo continuo de las economías y sociedades pasa por priorizar aquellas medidas que mejoren la productividad en todos los sectores industriales. Resulta especialmente interesante analizar cómo una institución pública como la Guardia Civil, que sitúa a las personas en el centro de su modelo de negocio, integra los principios de la economía social en su misión de garantizar la seguridad ciudadana.

Actualmente, la economía social ha sido impulsada por el Comité Económico y Social Europeo focalizando la interdependencia entre la economía y la sociedad. El concepto en España ha sido ampliamente difundido por la confederación Empresarial Española de la Economía social (CEPES). Es más, la ley 5/2011, de 29 de marzo en su Preámbulo, agrupa los principios de diferenciación en las entidades de la economía social, uno de ellos es: la focalización en las personas y objeto social, como principal. En este contexto, las organizaciones participantes acogen proyectos sociales realizados individualmente, como instituciones con otra forma jurídica (Sánchez et al., 2018). Alineado al Plan Integral de Cultura de Seguridad Nacional, por desarrollarse en concordancia con los Objetivos de Desarrollo Sostenible (ODS) marcados por la Agenda 2030. Este necesita para su evolución, la colaboración activa de todos los sectores que forman el ecosistema social, desde las organizaciones privadas hasta las públicas, pasando por las organizaciones de la sociedad civil, sin olvidar el sector académico (García-Flores & Palma, 2020).

Siguiendo el punto anterior, se podría decir que la institución de la guardia civil perteneciente al sector público presenta un enfoque integrado en la economía social a través de las dimensiones o capitales que forman su capital intelectual (CI). La Institución de la Guardia Civil desde su creación, basa sus acciones en la seguridad, la prevención y la protección de los derechos y libertades del ciudadano, pero también en su cuidado y auxilio, cuando se encuentran en una situación de vulnerabilidad (capital humano). En este sentido, fomenta la participación y coordinación a nivel interno y externo con diferentes entidades lo que se conoce como carácter benemérito (capital estructural). Este intangible, combinado con otros tangibles como la estructura y diversificación de la institución, no sólo sirven para fortalecer alianzas que fomenten redes sociales ya establecidas, sino también es empleado como facilitador de conexión entre comunidades e individuos alejados entre sí (Burt, 2004) (capital relacional). Sin olvidar que, la cohesión y la confianza generada en estas relaciones facilitan la transmisión del conocimiento, siendo un intangible valorado en la economía (Arteaga et al., 2020).

La investigación sobre el CI ha mostrado la relevancia valorativa otorgada. Garanina et al., (2021), en una revisión estructurada en diferentes países realizada en el periodo (2010-2020), observaron la convergencia de los investigadores a conceptualizar el concepto de CI como generador de valor empresarial. En este trabajo evitaremos entrar en la retórica sobre el valor de los intangibles vs. tangibles ya que hoy en día, se ha dejado atrás la controversia de los años 70 de la era postindustrial. En ella, el valor de los intangibles que tenía una empresa empezaba a ser tema de debate en los informes financieros. Del mismo modo olvidadas están, las controversias planteadas sobre ellos después del estallido de la burbuja de las empresas puntocom, la crisis financiera mundial

del 2008, donde las empresas empiezan a evaluar los "riesgos" y, un periodo de relativo estancamiento económico (Hazan et al., 2021).

La academia, nos indica que el paradigma del CI se considera asentado como sistema para la consecución de valor empresarial, entre los académicos a finales del año 2010 y, por tanto, ha alcanzado consolidación teórica en nuestros días. En consecuencia, el objetivo de este estudio consiste en analizar en qué medida las acciones solidarias y humanitarias de la Institución de la Guardia Civil generan valor social para los grupos de interés, impactando en la economía social a través de la gestión de los elementos que componen su CI, por ser clave para el crecimiento y desarrollo social (Haskel & Weslake, 2018; Stratone, 2023). Nuestra decisión está basada en cubrir un vacío encontrado en aplicar un enfoque de CI a una institución pública como agente activo en la economía social y estudiada tradicionalmente bajo el prisma operativo y jurídico. Al visibilizar estos principios en la Institución de la Guardia Civil pretendemos abrir otras líneas de investigación no tan exploradas en la economía social y en los cuerpos de seguridad nacionales e internacionales en su estudio sobre el CI.

El presente artículo está estructurado como sigue: en el primer apartado, realizamos una breve revisión y definición sobre el concepto de Capital Intelectual (CI). Seguidamente, en el segundo apartado, se analizan las sinergias entre la Economía Social y la institución objeto de nuestra investigación e inferimos nuestras hipótesis de investigación. Estas hipótesis quedan planteadas en el apartado tercero, versando sobre la metodología empleada. En línea a este último, el cuarto apartado, expone los resultados obtenidos de la investigación, finalizando con el quinto apartado sobre las conclusiones establecidas, aportaciones y limitaciones.

2. MARCO TEÓRICO

2.1. CAPITAL INTELECTUAL (CI)

Las empresas a nivel micro o macro en cualquier sector, deben considerar tanto sus activos tangibles como los intangibles útiles para la creación de valor, a lo que se le suele denominar capital intelectual (Cañibano, et al., 2002; Bueno et al., 2008; Fernández et al., 2022). Este adquiere prominencia, al quedar establecida la importancia de los intangibles en la economía empresarial, posicionando la inversión en activos intangibles frente a los activos tangibles. Existen estudios que demuestran, que estos son claves para el crecimiento económico y empresarial (Haskel & Weslake, 2018; Stratone, 2023), sobre todo debido a su aceleración después de la pandemia del COVID-19 (Hazan, 2021). No obstante, esto no siempre fue así, si revisamos los estudios anteriores sobre intangibles encontramos a principios de los años 90 la génesis del concepto de CI.

Después de la era post-industrial en los años 70, las empresas ya empiezan a preguntarse por los intangibles. Unas décadas más tardes, las economías globalizadas y en red de los años 90, demostraron la importancia del activo intangible que suponía contar con un flujo tanto interno como externo de información, conocimiento acumulado y procedimientos propios. Eran intangibles que no se reflejaban en los estados financieros, pero contribuían al logro de los objetivos de la empresa. Así, podemos decir que el CI surgió como resultado de querer conocer el producto resultante de restar el valor real de una compañía y su valor en el mercado.

Edvinsson y Malone (1999), intentan explicarlo con la metáfora de que el CI sería las raíces de un árbol, algo que no se ve, pero necesario para crecer. Para estos autores, está compuesto por la infraestructura, las relaciones con los socios y clientes y las habilidades de los empleados. Otros autores como Johnson (1999), enfatizan en ese grupo de intangibles, la inteligencia humana y la innovación como generadoras de beneficios. Una revisión de la literatura sobre el CI nos conduce a extraer las teorías influyentes como pilares de su desarrollo:

1. Teoría de los recursos y capacidades *(Resource-Based View, RBV)*. Barney (1991), postula que los recursos de una empresa para ser competitivos deben ser valiosos, raros, inimitables y no sustituibles, popularizando en la academia y en la práctica, el llamado criterio VRIN. Donde la estrategia empresarial, se focaliza en las prácticas y procesos comprendidos en la actividad diaria desarrollada en la organización y sus resultados (Potter, 1996). Está teoría empezará a conceptualizar no sólo los recursos tangibles, sino también los intangibles como el conocimiento (Grant, 1996).
2. Teorías basadas en el conocimiento (*Knowledge-Based View, KBW)*. En la nueva sociedad del conocimiento*,* este será el recurso por excelencia. Su mayor exponencial es la espiral del conocimiento, ampliamente popularizada por sus creadores Nonaka y Takeuchi (1995). Su visión de la empresa es como un ente activo de creación y difusión del conocimiento. Para ello, el conocimiento tácito, aquel que es inarticulado, intuitivo, surge del individuo con la experiencia "en" y "con" el trabajo que desempeña "*know how*" (Nonaka & Takeuchi, 2021). Se transmite a la vez que se transforma en la organización al ser aplicado (Grant, 1996) en conocimiento explícito. Este, puede ser codificado, escrito, objetivo y fácilmente transferido (Nonaka & Konno, 1998), el "*know about*", creándose a nivel organizacional e individual. Imprimiendo esta teoría un dinamismo y proyección exterior, de la que carecía la anterior (Bontis, 2002).
3. Teoría de las capacidades dinámicas. Como exponen sus precursores (Teece et al*.,* 1997) se centra en la capacidad combinatoria que tienen las empresas de que su conocimiento, habilidades y experiencia permanezcan integrada en sus productos y procesos siendo difíciles de imitar. Aunque más moderna que las expuestas en los puntos anteriores, se ha expandido en los siguientes campos: emprendimiento (Álvarez & Barney, 2001); desempeño empresarial (Wang et al., 2011; Stratone, 2023); retorno de inversión (Chen et al., 2009; Tan et al., 2007); entornos en red (Zheng et al., 2011) y medioambiente (Chen, 2008; Haarhaus & Liening, 2020).

Estas teorías dan como resultado definir el CI como el conjunto de recursos intangibles y tangibles y la capacidad de las empresas para gestionarlos, haciéndolas competitivas y sostenibles.

2.1.1. Definición y dimensiones del CI

En la revisión literaria no se ha encontrado una definición universalmente aceptada del CI. A pesar de ello, los autores coinciden en mostrar como su identificación y uso, crea beneficios para la organización (Hazan et al., 2021; Sumedrea, 2013). Exponemos las aportaciones de algunos autores relevantes, que han investigado el CI a continuación (tabla 1).

Tabla 1
Principales aportaciones a las definiciones del CI.

Aportaciones a la definición del CI	Autor
Sistemas y procesos que la hacen competitiva.	Steward, 1997
Los activos que no están en los estados financieros pero deberían reflejarse.	Petty & Guthrie, 2000; Roos, 2001 Reed et al. 2006; HernandezBueno et al., 2008
Fuente de futuros beneficios.	Lev, 2001
Necesarios para la innovación.	López et al., 2004; Rideg et al., 2023
Impulsor de la innovación y factor clave en la economía.	OECD, 2006
Combinación de intangibles y tangibles alineados a la estrategia empresarial para generar beneficios.	Bueno et al., 2008
Conocimiento a disposición de la organización para decidir las estrategias.	Aramburu et al, 2015
Creación de valor	Cañibano et al., 2002 Demartinni &Trucco, 2016 Garanina et al., 2021
Motor del desarrollo económico y social	Merino et al., 2018 Suciu & Năsulea, 2018
Creación valor corporativo y generación ventajas sostenibles en economías emergentes	Xu & Wang, 2018
Recursos estratégicos.	García-Flores & Palma., 2020
Motor de la cuarta revolución industrial.	Li et al., 2020
La tecnología es impulsora de las relaciones sociales que posibilitan su difusión.	Briñez, 2021
Rápido crecimiento económico.	Hazan et al., 2021
Efectos en el valor del mercado	Dumay et al., 2016
Mejora el desempeño organizacional	Thum-Thysen et al., 2021 Fernández-Solís et al., 2025

En este estudio definimos al CI como valores intangibles que, gestionados junto con los tangibles contribuyen al crecimiento empresarial, económico y social.

Así como no existe consenso sobre la definición de CI, tampoco existe un modelo universalmente aceptado para su medición. A lo largo del tiempo, diversos modelos han intentado clasificar la medida de los intangibles, evolucionando desde modelos más simples como el de Skandia (1997) hasta otros más complejos como el modelo actualizado Intellectus (2011).

Entre los pioneros en la medición del CI, el Navegador de Skandia de Edvisson y Malone (1997), agrupa los elementos que componen el CI en dos dimensiones para su estudio: capital humano y capital estructural. En cambio, en la mayoría de autores dedicados al estudio del CI, existe consenso en agrupar los intangibles que lo componen en tres capitales: capital humano (CH), capital relacional (CR) y capital estructural (CE) (Petty & Guthrie, 2000; Navarro & Medina, 2024). Para ejemplificarlo, exponemos las clasificaciones en capitales con sus elementos en la tabla 2. En la primera columna se muestran los indicadores de Johnson (1999) que aportó a la literatura, una clara distinción entre indicadores financieros y los no financieros en relación al valor del mercado de una compañía. La segunda columna muestra la clasificación realizada por Cañibano et al. (2002) basadas en el proyecto MERITUM[1] impulsado por la OCDE y la CE, se ha representado por estar la Institución enmarcada en este contexto.

Tabla 2

Ejemplos de clasificaciones de Categorías e Indicadores del CI.

Capitales	Elementos no financieros	Elementos CE y OCDE
Capital Humano (CH)	Habilidades; conocimientos; tareas y motivación	Capacidades, saberes, habilidades y experiencias
Capital Estructural (CE)	Procesos de negocio y renovación, flow de información, productos y servicios; formas de cooperación de procesos	Procedimientos, rutinas organizativas, cultura, sistemas, bases de datos, licencias, etcétera.
Capital Relacional (CR)	Relaciones con los socios, clientes, proveedores e inversores	Relaciones con clientes, proveedores, socios de I+D+i.

Para estos autores reseñados, el CI es la combinación de los elementos que forman los capitales que tienen las empresas. No obstante, en la revisión de la literatura también hemos encontrado autores como Delgado et al., (2008), que prefieren estudiarlo dividiéndolo en cinco dimensiones: capital humano, capital tecnológico, capital organizativo, capital relacional y capital social. Siguiendo esta última categorización del CI, se podría pensar por ello, la conveniencia de extraer del CI el capital social y alinearlo con la economía social. La objeción que planteamos sería que el capital social ya sea como dimensión o como subdivisión del capital relacional, en sí mismo no crea valor si no es con la interacción de los otros dos capitales, como explicamos a continuación.

Para ello, en este punto, pasamos a definir de forma sintetizada las dimensiones en las que se suelen categorizar los elementos que forman el CI por los académicos para su estudio, y como se encuentran relacionadas:

- La dimensión capital humano (CH), comprende los conocimientos establecidos en los empleados de una empresa; los individuos son capaces de generarlo (Delgado et al. 2008). Reside en las capacidades, habilidades, experiencia (Bueno & Merino, 2007; Bellucci et al., 2021), valores y actitudes hacia la empresa y el puesto de trabajo. Además, este capital recoge el de los colaboradores por ser

[1] Measuring Intangible to Understand and Improve Innovation Management (MERITUM): Proyecto conjunto entre la OCDE y la CE para impulsar la investigación en Europa (1998-2001).

ORCID: Https://orcid.org/0009-0000-2569-3710

fuentes activas de conocimiento útil, para la organización (Merino et al., 2018). La relación con los otros dos capitales se manifiesta tanto en la innovación (Li et al., 2020), por ser los individuos de una organización los que solicitan nuevas formas de hacer las cosas (CE) como en la capacidad para trabajar con otros y negociar, lo que requiere motivación, lealtad y satisfacción (CE, 2006) (CR).

- La dimensión capital estructural (CE), está constituida para la mayoría de los autores (Chen et al., 2009; Delgado et al., 2008; Dumay et al., 2016; Merino et al., 2018, Oliveira et al., 2020) por activos como: la estructura organizacional, las rutinas, procedimientos, procesos, bases de datos, manuales, patentes y software, que permanecen en la empresa cuando los individuos que trabajan en ella han finalizado su trabajo. Algunos de ellos son tangibles como: la maquinaria y la estructura. Sin embargo, otros son intangibles como la propiedad intelectual, la marca registrada, las patentes, la cultura organizacional (Chen et al., 2009) y la imagen (Merino et al., 2018; Jeffrey et al., 2019). La relación más reseñable con los otros dos capitales está basada en la estructura que presenta la organización. Esta, sirve de andamiaje por donde transfieren los procesos y procedimientos entre el capital humano y tecnológico creando relaciones entre los grupos de interés o *stakeholders*[2].

- La dimensión capital relacional (CR), abarcaría los activos generados por el conjunto de relaciones entre los empleados, los clientes, los proveedores, accionistas (Bellucci et al., 2021), las alianzas estratégicas que generan información y los conocimientos relevantes para la empresa. La sinergia generada con los otros capitales la podemos ejemplificar con relaciones formales e informales, entre los empleados en la organización, por ser claves en la transmisión y generación de información y conocimiento (CH). Con el CE, lo vemos a través de que este conocimiento se difunde de unos individuos a otros y también se transforma permaneciendo en las organizaciones (De Castro & García, 2003), influyendo en la economía y en la sociedad (Garanina et al., 2021). La importancia de este capital relacional se percibe en la segmentación de clientes que las empresas suelen hacer; creando o disminuyendo acuerdos comerciales y estableciendo o fortaleciendo alianzas, ya que no todos tienen las mismas necesidades o estas cambian con el tiempo.

De esta forma, es la interacción de los capitales mencionados la que crea valor en una organización. La ejemplificamos con la generación de conocimiento, por ser reconocido como clave para el desarrollo económico (OCDE, 2006). La información y el conocimiento se difunde a través de unas estructuras (Devenpor & Prusak, 2001; Wang, 2011) humanas, o tecnológicas o ambas (CH). También sabemos que se acumula en ellas a través de procesos, operaciones, rutinas organizacionales, procedimientos, etcétera (De Castro & García, 2003), estas son el andamiaje para las actividades comerciales y sociales, consiguiendo valor organizacional (Demartinni & Trucco, 2016) (CE). Pues bien, en mayor o menor medida se fomenta el desarrollo de una red, que promueva esquemas de participación, colaboración, desarrollo de iniciativas y plataformas sociales

[2] *Stakeholders*. Para el pionero Friedman los *Stakeholders* son cualquier tipo de personas que influye o es influido por una empresa. Entre los grupos de interés de la Guardia Civil nos encontramos a la ciudadanía, las administraciones públicas, los guardias civiles y otras organizaciones como ONGs, seguridad privada, universidades y cuerpos policiales internacionales. Dentro de estos también se encuentran personas con intereses opuestos que pertenecen a: bandas criminales, grupos terroristas, delincuentes, etcétera.

(CR). No obstante, esta red aún en su óptimo estado podría entorpecer la fluidez del conocimiento, debido a los elementos que la componen, como: disponer de personal insuficiente o pésimo, mala gestión, o incluso que, los procedimientos o políticas de estrategia de la empresa, interfieran negativamente en ella (Merino et al., 2018).

Como conclusión teórica, no cabe duda que la focalización sobre el valor real de una empresa y determinarlo, fue el *driver* del desarrollo del capital intelectual. Se trataba de explicar el resultado de la diferencia encontrada entre el valor de una compañía en sus libros financieros, y su valor en el mercado. Este valor explicado al CI, se debe a la interacción de los elementos que lo forman como son: las habilidades, conocimiento y experiencia de los empleados junto con los proyectos en I+D+i; las rutinas organizacionales; la interacción de relaciones internas y externas (Briñez, 2021) tanto a nivel empleado como con los proveedores, accionistas, aliados y clientes (CE, 2006)[3]. Sin olvidar, la gestión de transformarlos, adquirirlos y aplicarlos en un entorno cambiante (Nonaka & Takeuchi, 2021).

Estas características, posicionan al CI como clave para el crecimiento económico (Bellucci et al*.,* 2021), social y sostenible (Secundo et al., 2020) adaptado a un mercado volátil, difuso, incierto, ambiguo, complejo (Nonaka & Takeuchi, 2021) y en disrupción tecnológica (Wang et al*.,* 2021). Debido a ello, en el siguiente apartado exponemos empíricamente, a través de la Institución de la Guardia Civil, como las empresas, pueden aportar beneficios económicos sociales a través del CI.

2.2. ECONOMÍA SOCIAL Y EL CUERPO INSTITUCIONAL DE LA GUARDIA CIVIL

La economía social[4] es definida como un conjunto de actividades empresariales y económicas, realizadas por entidades para la consecución del bien colectivo de sus integrantes, el interés general económico y/o social siguiendo los principios de la economía social (MITES, 2025). Actualmente, el concepto en España está consolidado, encontrándose difundido por el Centro Internacional de Investigación e Información sobre la Economía Publica, Social y Cooperativa. Si relacionamos estos términos: público, social, cooperativismo y economía pública nos lleva a pensar en una organización que los ha alineado en su estrategia durante más de 181 años de existencia: la Institución de la Guardia Civil, al converger prácticas económicas y sociales en la provisión de bienes y servicios. Nos basamos, al encontrar en la Institución, principios establecidos de la economía social y colaborativa como los enumerados a continuación, por autores como Díaz- Foncea et al., (2016):

- Promover la solidaridad entre los empleados facilitando estructuras, motivándolos a ser solidarios y a la cooperación.
- Reconocimiento del trabajo solidario y comprometido a través del espíritu benemérito.
- Promoción de la igualdad en un sentido amplio no sólo basada en el género.

[3]Documento RICARDIS de la UE (2006). La Comisión Europea, se apoya en esta interacción basada en el proyecto MERITUM, 2002. Se define como la combinación de recursos y actividades de capital humano, capital estructural y capital relacional de una organización.

[4]Actualmente, es impulsada por el Comité Económico y Social Europeo focalizando la interdependencia entre la economía y la sociedad.

ORCID: Https://orcid.org/0009-0000-2569-3710

- Inclusión y cohesión social.
- Ayudar y apoyar a los colectivos más vulnerables y en riesgo de exclusión social.
- Conciliación de la vida profesional con la familiar.
- Generar sostenibilidad a nivel interno y externo, con claro respeto al medioambiente y la protección de la biodiversidad.

La ventaja competitiva de esta Institución, es ofrecer servicios de calidad superior para ser referente en su sector, ante los ciudadanos, el estado y la Unión Europea. Queda establecida como su misión, dentro de los Cuerpos y Fuerzas de Seguridad del Estado el "*proteger el libre ejercicio de los derechos y libertades y garantizar la seguridad ciudadana*" (Art. 104, Constitución). Lo hace situando a las personas en el centro de sus actuaciones, velando por su seguridad e integridad, de forma cercana. Las funciones quedan determinadas en la tabla 3.

Tabla 3

Definición de las competencias funcionales de la Guardia Civil

Nota: Los datos recogidos en esta tabla está basada en la Ley Orgánica 8/1986 de 13 de marzo y en las Memorias de Sostenibilidad de la Guardia Civil, 2023.

Diferentes Cuerpos de Seguridad Artículo 11 (página 26)	Específicos de la Guardia Civil Artículo 12, B (página 27)
• Velar por el cumplimiento de las leyes y disposiciones generales. • Auxiliar y proteger a personas y bienes. • Vigilar y proteger edificios públicos. • Mantener el orden y velar seguridad ciudadana. • Prevenir la comisión de actos delictivos. • Investigar delitos, asegurar las pruebas e instrumentos poniéndolos a disposición del juez. • Prevención de la delincuencia. • Colaborar con Protección Civil, caso grave de riesgos o catástrofes.	• Control de armas y explosivos. • Resguardo Fiscal del Estado (costas, fronteras, puertos y aeropuertos) • Vigilancia del tráfico, tránsito y transporte en las vías públicas interurbanas (exceptuando el País Vasco y Cataluña). • Conservación de la naturaleza y medioambiente, recursos hidráulicos, riqueza forestal y de otra índole relacionada con la naturaleza. • Conducción interurbana de presos y detenidos. • Aquellas otras que les atribuye la legislación vigente.

Adicionalmente a las funciones presentadas en la tabla superior, al compartir competencias con otras policías autonómicas y nacionales, la Guardia Civil es responsable de la seguridad ciudadana en el 84,53% del territorio nacional y del mar territorial (GC, 2023). Por otra parte, al ser un cuerpo de seguridad pública de naturaleza militar, puede desempeñar misiones internacionales integrándose tanto en una organización internacional como EUROPOL, la ONU o la OTAN, así como en las Fuerzas Armadas españolas (GC, 2023).

Podemos decir que, con más de 80.000 efectivos, desplegados por todo el territorio nacional e internacional. Se diversifica en especialidades: Protección a la naturaleza, Policía Judicial, Servicios de Información y Servicio Marítimo, entre otras. Junto con, el

potencial humano desplegado en seguridad ciudadana, contando con más de 2.000 unidades territoriales (GC, 2025).

2.2.1. Valor social creado por la Institución.

El valor social, lo podemos definir como el resultado positivo de las acciones desarrolladas por una entidad sobre la sociedad (Retolaza & Alzola, 2021). Este intangible, esta contextualizado en el compromiso de los guardias civiles a ir más allá del cumplimiento de su misión. Lo hacen como contribución social, focalizándose tanto en mejorar la vida y apoyo a los ciudadanos, como siendo conscientes de las preocupaciones ambientales, siguiendo uno de los principios de la economía social planteados por Díaz y Lejarriaga (2019). Por ejemplo, respecto a este último principio, ha registrado la huella de carbono en la Oficina Española de Cambio Climático (OECC), convirtiéndose en uno de los únicos cuerpos policiales en hacerlo a nivel mundial. Reseñamos también, el premio concedido por las Naciones Unidas en el año 2023, "Premio Protección del Ozono para agentes de Aduanas y Policías".

Estos valores son potenciados por la Institución a través de la transparencia y el reconocimiento de sus actuaciones, presentando un impacto integrador y de colaboración, donde las comunidades en donde se desarrollan sus proyectos tienen un rol en la toma de decisiones, sobre qué consideran como valor. Por consiguiente, la Institución combina sus recursos, políticas y procesos para conseguir mejoras en las vidas de las personas y de la sociedad en general, que es como se denomina al valor social (Retolaza & Alzola, 2021).

Para desarrollar sus capacidades, su modelo de negocio es difundir y aplicar una cultura de seguridad de calidad, versátil, disponible y cercana al ciudadano. Lo realiza transmitiendo sus conocimientos y experiencia a otros cuerpos policiales nacionales e internacionales, a los ciudadanos, al gobierno y a otros grupos de interés, con profesionalidad y carácter benemérito. Esto último es reconocido porque los guardias civiles trabajan con el conocimiento y el compromiso de hacer cosas extraordinarias, coadyuvándose en lo que hemos llamado intangibles.

Recordemos que en el primer Reglamento para el Servicio del año 1.844 en su art. 32, ya constaba su carácter benéfico y protector. En las mismas fechas, quedaba expresado en el art. 6º de la Cartilla del Guardia Civil, la atención a las personas desprotegidas y ser, pronóstico feliz para el afligido (GC, 2025). Unos años más tarde en el año 1.929, se le concedía a la Institución la Gran Cruz de la Orden Civil de la Beneficencia con distintivo blanco y negro que implica riesgo personal, en reconocimiento a los servicios humanitarios y heroicos realizados. Por consiguiente, podemos decir que la solidaridad y cooperación son valores establecidos en el ADN de la Institución al ser generado desde su creación, convirtiéndose en seña de identidad del Instituto.

El espíritu o carácter benemérito, sigue presente en la actualidad, expresado en su Código de Conducta[5]. Su artículo 21, establece la prestación de auxilio a los ciudadanos, encontrándose su personal o no de servicio. También, lo encontramos en el decálogo de los miembros de la Guardia Civil en su punto 7, al expresar este apartado, la de ayudar

[5] Real Decreto 176/2022 de 4 de marzo, por el que se aprueba el código de conducta de la Guardia Civil.

siempre a quienes más lo necesitan incidiendo en las personas en situación de desprotección y vulnerabilidad; también se expresa a través de sus memorias de responsabilidad social corporativa (MRSC) y en la revista oficial de la Guardia Civil.

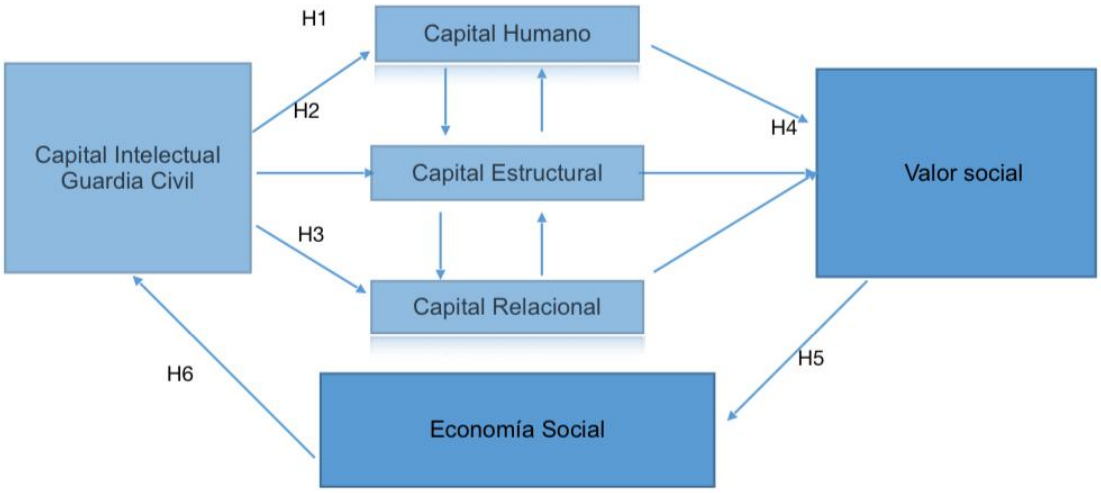
Por lo tanto, este intangible es potenciado por la Institución, considerándose un activo organizacional, impulsándolo a través de los servicios humanitarios, el voluntariado, la lucha por la biodiversidad y el medioambiente. Produciéndose, tanto a nivel individual o en otras organizaciones, como queda recogido en su página web #GComprometidos.

Por todo lo expuesto, podemos decir que la misión de la Guardia Civil no se basa únicamente en seguridad pública sino también incluye el bienestar de la sociedad, quedando determinado a través del dinamismo que aporta las dimensiones del CI que lo forman, generando crecimiento económico (Nonaka & Takeuchi, 2021). Sin embargo, este valor económico-social no es tenido en consideración o es desconocido por la academia ya que, al realizar nuestra investigación, no se han encontrado estudios, investigación o artículos que versen sobre ello. Por ello, en el siguiente apartado expondremos nuestras hipótesis sobre la contribución del valor económico social de la Institución, en el modelo de investigación.

3. METODOLOGÍA

En base a lo anterior presentamos el modelo de investigación (Figura 1) donde se exponen las hipótesis de este estudio:

Figura 1.
Modelo de investigación e hipótesis.



H1. El Capital Humano está identificado en la Institución.

H2. El Capital Estructural está identificado en la Institución.

H3. El Capital Relacional está identificado en la Institución.

H4. La interrelación de los tres capitales impacta en la creación de valor social.

H5. El valor social generado influye en la economía social.

H6. La economía social influye en el capital intelectual de la Guardia Civil.

Al objeto de contrastar nuestras hipótesis, hemos seguido las indicaciones de Codina et al., (2020) realizando una revisión literaria usando bases de datos científicas como: SCOPUS, Web of Science y Google Scholar. Estos autores muestran en su investigación que estas bases de datos, usadas por la comunidad científica internacional, recogen ampliamente todas las áreas de conocimiento. La búsqueda se ha realizado tanto en los campos: títulos de artículos, en el *abstract* o por las palabras claves indicadas en este artículo. Sin embargo, la consulta no ha devuelto ningún resultado, demostrando la falta de artículos científicos que versen sobre nuestro tema de investigación. Debido a ello, nuestros datos han sido obtenidos de la revisión documental y bibliográfica de bases de datos del Ministerio del Interior, así como del Ministerio de Defensa y de la Institución de la Guardia Civil, donde la Institución pública sus informes financieros y no financieros. Nos basamos, por tanto, en datos cuantitativos y cualitativos de fuentes primarias en abierto.

La técnica elegida ha sido un análisis de contenido[6] por ser frecuentemente usada con éxito, en el análisis de los informes de divulgación del CI (Magau 2021; Dumay el al., 2016). Igualmente, es apropiada para verificar hipótesis planteadas deductivamente (Bini & Giunta, 2017). El corpus del análisis de contenido, son las Memorias de Responsabilidad Social de la Guardia Civil (MRSCGC) y Memorias de Sostenibilidad (MS). Nuestra decisión está sustentada en que los informes anuales son herramientas empleadas por las organizaciones para comunicar a todos los grupos de interés lo que consideran importante, divulgándolos en ellos (Petty & Guthrie, 2000; Bontis 2002; Guthrie & Abeysekera, 2006; Dumay et al., 2016). Alineado a que la tendencia actual seguida por las compañías es divulgar en estos informes anuales, sus estados financieros y no financieros a los grupos de interés (Dumay et al., 2016).

Es un estudio longitudinal abarcando el periodo comprendido entre el año 2014 y el año 2023, fecha de los últimos informes de información anual divulgados. Con ello además de determinar la consistencia de los datos, conseguimos obtener la tendencia institucional analizando los mismos. Pretendemos responder, si la contribución de la institución, a la economía social es inherente en ella, siguiendo nuestro objetivo de estudio.

La unidad de análisis en los análisis de contenido, es la que indica la presencia o ausencia de los elementos a investigar (Moreiro et al., 2006). Para obtener esta unidad de análisis, entre los marcos conceptuales usados para definir, clasificar y registrar la información divulgada sobre el CI, algunos autores suelen emplear el modelo de Sveiby (1997) modificado por Petty y Guthrie (2000). Sin embargo, en esta investigación, para

[6] Para Allport (1965), se trata de un método para estudiar y analizar las comunicaciones de forma sistemática, objetiva y cuantitativa con el objetivo de medir variables.

obtener nuestra unidad de análisis hemos adaptado los indicadores del modelo Intellectus[7] (2011) a la Institución, por su amplia repercusión nacional e internacional y ser considerado un modelo integrador de medición del CI (Merino et al., 2018). Las consideraciones más notables de este modelo, son:

- La creación de un "árbol de pertinencia" estableciendo una estructura del CI, para identificar las unidades de medida que lo componen, estableciendo de forma jerárquica componentes, elementos, variables e indicadores. En base a ello, han sido elaboradas las categorías, los elementos, sus definiciones, y adaptado sus indicadores para la identificación del CI en la Institución (Ver Anexo I: tablas 4-6)

- La elaboración de un Índice Sintético, a partir de los componentes principales para cuantificarlo. Estos están representados en un "mapa de variables e indicadores principales" que será empleado como medida cuantitativa del conjunto de intangibles identificables. Siguiendo este punto, indicamos en el Anexo II, las fórmulas empleadas para la obtención de los índices.

- La elaboración del Informe de CI (ICI), para su difusión. Por consiguiente, siguiendo la literatura, se ha realizado una revisión de los documentos donde la Institución divulga sus informes financieros y los no financieros.

Se ha conseguido limar la subjetividad que podría efectuarse en la obtención de la unidad muestral o de análisis, añadiendo transparencia en la categorización y empleando reglas de decisión consistentes, a lo largo de nuestro estudio longitudinal. En relación a la fiabilidad, el instrumento de codificación ha sido manual sin empleo de software, evitando los problemas presentados por las palabras con múltiples significados que, aunque se puedan reducir aumentando las palabras claves en contexto, no detectan el significado del CI específico de la institución, o la interpretación que es realizada sobre él (ver Anexo III: Fases en el análisis de contenido).

Seguidamente, para conocer el comportamiento de nuestras variables de estudio (dimensiones del CI), se ha categorizado siguiendo la división tripartita del CI: capital humano, capital relacional y capital organizacional. Nos basamos en ella al haber sido establecida por la Comisión Europea (2006), basadas en el proyecto MERITUM (Cañibano et al., 2002) citado en el apartado 2.2. (ver Anexo I: tablas 4-6).

Finalmente, se ha realizado un análisis estadístico de las medidas de distribución de frecuencias, tendencias y dispersión. Mediante el estudio estadístico se pretende observar la importancia de los elementos para la Institución y su comparación y posición respecto a los demás elementos del CI, a lo largo de período estudiado. Para ello se ha usado el programa estadístico RStudio, versión 2024.12.0+467 para macOS 13+.

[7] Documento Intellectus, nº5(2003): Se gestó por el profesor Bueno y el Centro de Investigación sobre la Sociedad del Conocimiento (CIC). Se modificó en el 2011 dando lugar al Modelo Intellectus: Medición y Gestión del Capital Intelectual, por el IADE (Instituto de Administración de Empresas). Los indicadores adaptados están recogidos de su punto 6. : Cuadro de Indicadores (pp. 36-58).

4. RESULTADOS Y DISCUSIÓN

Los resultados de nuestra investigación identifican el CI en la Institución. En el análisis de nuestra investigación adaptando el modelo Intellectus, se desprende al construir las categorías, los elementos y los indicadores, la identificación de sus elementos componentes. El CI de la Institución se puede clasificar agrupando los elementos que lo componen en capital humano, capital estructural y capital relacional (ver Anexo I). Estos resultados arrojan similitud con la mayoría de los estudios académicos. En consecuencia, aceptamos las tres primeras hipótesis de esta investigación:

H1. El Capital Humano está identificado en la Institución.

H2. El Capital Estructural está identificado en la Institución.

H3. El Capital Relacional está identificado en la Institución.

Seguidamente, pasamos a verificar las restantes hipótesis. En referencia al valor social, al analizar la temática de los elementos que forman los capitales del CI y los capitales de la Institución (Anexo I) apreciamos en las definiciones de los elementos que componen el capital humano, el relacional y el estructural una incidencia directa al valor social. Es decir, los elementos del CI están alineados a la identificación de valor social recogido en la literatura como queda expuesto a continuación en la tabla 7.

ORCID: Https://orcid.org/0009-0000-2569-3710

Tabla 7

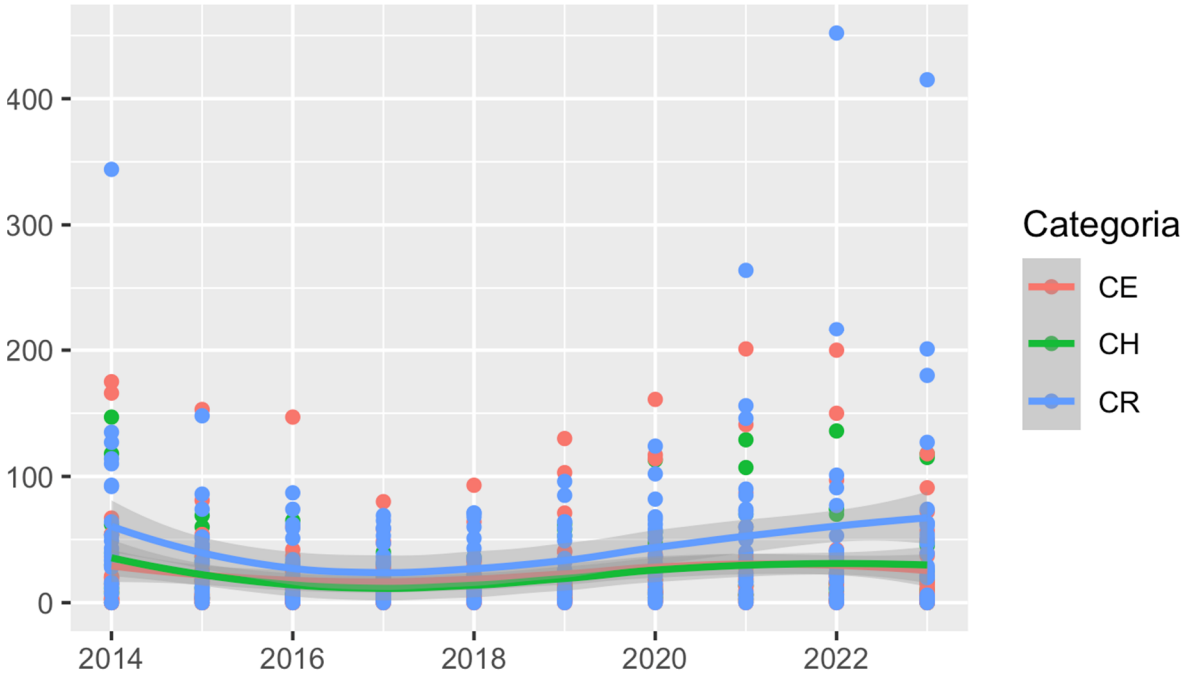
Relación entre el CI de la institución y el valor social.

Dimensión Capital Humano			
Elementos	Definiciones	Capital Humano	Valor social
IDENTIDAD MOTIVACIÓN CREATIVO EDUCACIÓN ESPECIALIDAD; UNIVERSITARIO FORMACIÓN EXPERIENCIA DESARROLLO APRENDIZAJE CIVIL CONCILIA LIDERAZGO	Valores, motivación a la excelencia en sus actuaciones, formación especializada y conocimientos. Adaptación y generación ideas novedosas aplicables en el desarrollo del trabajo.	Autores como Nonaka y Takeuchi (2021) puntualiza que las empresas que cuentan con empleados con muchas habilidades y experiencia son capaces de gestionar escenarios cambiantes. Capacidad sin actitud o aptitud generaría una desaceleración o destrucción del valor (Merino et al., 2018)	Valor aportado por las personas a las empresas (Carina et al., 2024). Las creencias personales sobre un propósito social (Díaz-Foncea et al., 2016).
Dimensión Capital Estructural			
Elementos	Definiciones	Capital Estructural	Valor social
CULTURA CLIMA IGUALDAD ESTRUCTURA DESARROLLO RUTINAs RELACIONINT CRIMINAL PROVEEDORES INVERSIONIDi PERSONALIDi INFRAESTRUCTURA EQUIPOPOLICIAL INNGEST COMUNICACIONGC MARCA LICENCIAS SECRETO PATENTES TECNOEXT TECNONEW TECLIC PLEXBIBILIDAD TALENTOS	Cultura institucional, idiosincrásica de la institución. Espíritu benemérito transferido generación a generación a través de acciones solidarias de cooperación, sacrificio y apoyo al necesitado. Seguridad y protección según la legislación vigente. La estructura de la Institución la hace distintiva, por su diversificación tanto geográfica como en especialidades para llegar a todos los ciudadanos. Andamiaje a través del cual el conocimiento, la experiencia y la información se transfiere diversificándose en especialidades aumentando así su valor empresarial. Sin olvidar las políticas e inversión en innovación y desarrollo.	Las empresas deben desarrollar su capital humano con los medios necesarios que apoye la visión sobre lo que las personas son capaces de hacer para generar cambio (Mohdzaini, 2021).	Recursos que los individuos pueden conseguir a través de la estructura de una organización (Sánchez et al., 2018). Sin estructuras sociales es difícil generar el capital social (Nonaka &Takeuchi, 2021).
Dimensión Capital Relacional			
Elementos	Definiciones	Capital Humano	Valor social
CIU LEALCIU QUEJAS PROTCIU ESTADO IADMINISTRACIÓN CAPITALEXTERIOR ALIANZAS ALIANZASESTABLES ALIANZASBENEFICIO CONCOMPETENCIA PRIVADA CERTICAL REDES ADMINISTRACIÓN MEDIOS DEFENSAMBIENTE VERDE MERCADO CODIGOCON ACSOCIAL BUENGOBIERNO	Genera valor a través de las relaciones y alianzas establecidas con todos sus grupos de interés. En el plano internacional, establece relación de cooperación y colaboración con otros países. Es reseñable el apoyo a los más vulnerable y desfavorecidos. La inclusión y la cohesión social. Impulsa proyectos de voluntariado dentro y fuera de la institución. Dedicada a la defensa del medioambiente interna y externamente y la biodiversidad. Cuenta para ello con una red de medios de comunicación internos y externos promoviendo la transparencia y el buen gobierno.	Las empresas generan valor a través de las relaciones creadas con sus grupos de interés (Maqbool,2020) y en la transmisión de ese conocimiento (Rideg et al. 2023; Nonaka & Takeuchi, 2021). Este conocimiento debe ser fluido (Merino et al., 2018).	A través de promover el empleo, la inclusión social, sostenibilidad, innovación y crecimiento económico se consigue impulsar la economía social (cepes, 2023). Las empresas logran sus objetivos sociales promoviendo la transparencia (Sumedrea, 2013). Los programas de inclusión económica tienen un fuerte impacto en las personas más pobres del mundo (Word Bank, 2024).

Una vez cuantificados los datos (anexo II) para conocer el comportamiento de los elementos de nuestras variables y si son una constante en el periodo estudiado, se ha efectuado un análisis de las medidas de distribución de frecuencias y tendencias (Figura 2).

Figura 2

Distribución de frecuencias y tendencias de los elementos del CI (2014-2023)



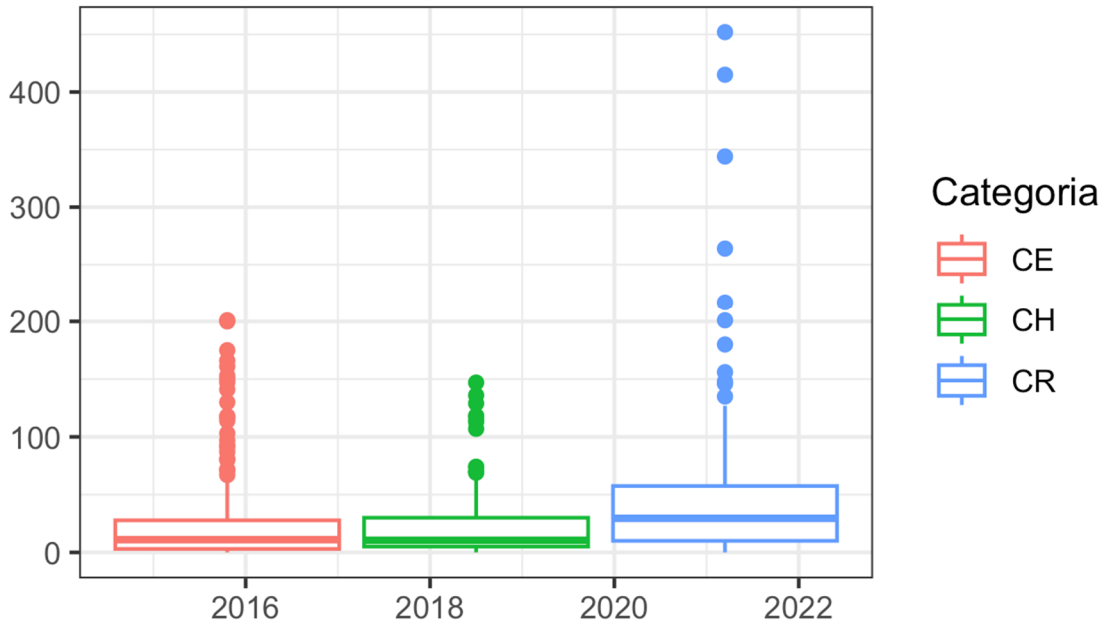
Observamos en la figura 2, cómo los elementos están representados en el periodo estudiado, y su distribución en categorías. Es reseñable que, mientras la curva de dispersión del capital humano (CH) y estructural (CE) se encuentran casi alineadas en los 10 años, señalando la constancia entre las frecuencias de los elementos de ambos capitales, la del capital relacional (CR) se mantiene por encima de las mismas. Sumado a que, las puntuaciones atípicas de los elementos de este último capital, son las más alejadas en comparación con la de otros dos capitales en los últimos años, mostrando la relevancia de esos elementos.

Seguidamente, para conocer la agrupación de esos elementos, en la figura 3, se han empleado medidas de tendencia central y posición. Se ha elaborado un diagrama de cajas que visualice tanto las medidas de posición central (media, mediana y moda) y las medidas de posición no centrales, cuartiles, basándonos al conocer por la figura 2, la dispersión de los datos.

ORCID: Https://orcid.org/0009-0000-2569-3710

Figura 3

Diagrama de medidas de tendencia central dimensiones del CI (2014-2023).



Al observar (figura 3) la dispersión de los datos y las puntuaciones atípicas, escogemos como medida de posición central la mediana. Este gráfico, nos muestra que la mediana del capital relacional se encuentra por encima del Q3 de los otros dos capitales, y que su rango intercuartílico es casi el doble, unido a las líneas que sobresalen por el margen superior de la caja (bigotes) y la distancia que hay entre sus puntuaciones atípicas, confirmando la dispersión de los datos. Observamos puntuaciones muy superiores en el capital relacional en el 50% de sus puntuaciones, superiores a los otros dos capitales, junto a que sus puntuaciones atípicas son las más elevadas en el periodo estudiado. Esto último, es interesante al significar la importancia que la Institución concede a esos datos atípicos. Un análisis desglosado sobre esas puntuaciones atípicas, nos indican que corresponden a los elementos detallados en la tabla 8.

Tabla 8

Puntuaciones atípicas de los elementos en el periodo estudiado

Elemento	Total 2014	Total 2015	Total 2016	Total 2017	Total 2018	Total 2019	Total 2020	Total 2021	Total 2022	Total 2023
CRALIANZASESTABLES	X								X	
CRALIANZASBENEFICIO	X	X	X	X						
CRPROTCIU		X			X	X	X	X	X	X
CRACSOCIAL	X			X	X	X		X	X	X
CRVERDE		X	X			X	X	X		X
CRDEFENSAAMBIENTE	X							X		X
CECRIMINAL	X	X	X		X	X	X	X	X	
CECOMUNICACIONGC	X	X	X	X	X	X	X	X	X	X
CEIGUALDAD						X	X	X	X	X
CHFORMACION	X	X	X			X				
CHDESARROLLO		X			X	X	X			
CHUNIVERSITARIO						X	X	X	X	X
CHCREATIVO								X	X	X

La tabla 8, muestra la relevancia de los elementos por haber obtenido mayores puntuaciones: Alianzasestables, Alianzasbeneficio, Protciu, Social, Verde, Defesaambiente, dentro del CR. Los elementos: Criminal, Comunicaciones, Igualdad, dentro del CE y los elementos: Formación, Desarrollo, Universitario y Creativo, dentro del CH. Destacando las puntuaciones elevadas de los elementos: Protciu junto con Asocial durante 7 años, Criminal durante 8 años, y Comunicación durante 10 años.

Con estos datos (tabla 8) y las unidades muestrales (anexo I) inferimos que para la institución sus acciones se dirigen tanto a la seguridad, como a la protección de los ciudadanos y al desarrollo de acciones sociales a través de la solidez de las alianzas y servicios conjuntos con otras identidades. En la misma línea, sus acciones van desempeñadas a la protección del medioambiente y la biodiversidad. Para ella, el "valor" no se considera solamente en términos financieros sino en línea con Nonaka y Takeuchi (2021) lo "social y ambiental", también son activos valiosos, siendo constante en ello. Para ello su capital humano es igualitario y diverso, está cualificado y desarrollado, adaptándose y creando ideas nuevas en el desempeño del servicio transfiriendo su conocimiento.

Estos resultados nos demuestran que sigue la definición de valor social como resultado generado de la combinación de los recursos, procesos y políticas que mejoran la vida de las personas y a la sociedad en su conjunto (Sánchez et al., 2018). Por consiguiente, vemos queda corroborada la hipótesis 4:

H4: La interacción de estos capitales genera valor social.

Siguiendo nuestra línea de investigación seguidamente vamos a conocer cómo este valor social impacta en la economía social, más allá de su misión principal expuesta en el apartado 2. Para ello, se ha efectuado un análisis cuantitativo de datos obtenidos de nuestro corpus muestral, de elementos específicos como son: Protección y Acción Social al ciudadano (tabla 9), siguiendo los principios de la economía social y la definición de valor social.

Tabla 9

Indicadores de los elementos: protección y acción social al ciudadano.

	2022	2021	2020	2019	2018	2017	2016	2015	2014
Acciones beneficio comunidad (más allá misiones encomendadas).	1.012	960	1.151	2.659	2.647	2.986	1.956	1.318	1.620
Acciones solidarias (voluntariado nivel individual hay constancia).	1.026	267	347	121	114	140	215	180	62
Actividades de acercamiento a la sociedad	247	499	503	482	340	316	105	904	142
Charlas en centros escolares	34.459	21.328	16.078	34.848	12.970	12.412	16.245	12.814	11.782
Acciones seguridad mayores	3.607	2.740	3.275	3.732	3.816	3.769	9.712	10.364	11.605
Colaboraciones convenios.	261	149	106	114	92	86	96	115	95
Servicios humanitarios	242.575	218.303	215.697	194.923	193.593	193.135	458.360	167.266	SD

ORCID: Https://orcid.org/0009-0000-2569-3710

Los datos representados anteriormente (tabla 9), son interesantes al indicarnos que en los últimos nueve años han sido efectuados: 1.883.862 servicios humanitarios; 14.689 acciones en beneficio de la comunidad y 2.410 acciones voluntarias. Sumado a otras actividades solidarias y de protección a los mayores y menores. Demostrando que, las personas son más importantes que el capital en la economía social (Pedreño, 2024).

Estos datos señalan que los servicios humanitarios, y las acciones en beneficio de la sociedad son un plus. Además, su valor financiero es inestimable. Para visualizar el valor económico de estas acciones lo hemos sintetizado tomando como ejemplo el de la Asociación Guardias Civiles Solidarios [8] (ASGS). La tabla 10, representa el valor económico de sus actuaciones en los últimos 5 años, cuyos datos han sido obtenidos de las memorias de la ASGC.

Tabla 10

	Actuaciones	Niños	Adultos	Alimentos (kg.)	Valor económico €
Memorias 2024	60	2.977	2.987	22.540	60.257
Memorias 2023	44	4.771	9.109	44.980	45.396
Memorias 2022	65	1.832	63.396	362.040	367.356, 21
Memorias 2021	54	2.419	5.346	13.210	52.000
Memorias 2020	138	2.017	13.251	8.262	38.482

Valoración económica actuaciones "Guardias Civiles Solidarios"

Con los datos expuestos en ambas tablas (8 y 9) nos adentramos en la disciplina de la economía social que impregna a la economía tradicional, el valor de lo social (Diaz-Foncea et al., 2016) y a la institución de la Guardia Civil que la sustenta, a través de su capital intelectual. Con ello, queda demostrado que el valor de los servicios prestados impacta positivamente en la economía social al perseguir el interés general económico y/o social. Por consiguiente, la hipótesis 5 de nuestra investigación queda contrastada:

H5: El valor económico social de la institución influye en la economía social.

Finalmente, se ha analizado si la economía social revierte en la Institución terminando con ello el cumplimiento del objetivo de nuestra investigación. Para ello, hemos analizado la confianza otorgada a la Institución por los ciudadanos, instituciones y diversas entidades realizadas por el Centro de Investigación Sociológicas (CIS), durante el periodo estudiado. Los resultados aparecen a continuación en la tabla 11.

[8]Con el objetivo de canalizar las numerosas acciones individuales del personal voluntario en el año 2014, se fundó la Asociación Guardias Civiles Solidarios (ASGC)

Tabla 11
Valoración de la institución por la sociedad española

	2023	2022	2021	2020	2019	2018	2017	2016	2015	2014
Posición entre instituciones más valoradas	SD	FFCCSE	FFCCSE	FFCCSE	1ª	1ª	1ª	1ª	1ª	1ª

Como vemos, una valoración positiva revierte en la Institución a través de la lealtad y confianza que le procesa la sociedad. Al ser reconocida como una Institución con valor social, aumenta de forma significativa su reputación (Jeffrey et al., 2019; Maqbool et al., 2018). Dentro de la institución, el compromiso adquirido por los guardias civiles con la sociedad favorece la autoestima y la motivación al luchar por los derechos humanos y los más desfavorecidos (MS, 2023). Estas acciones, programas o proyectos de voluntariado están alineados hacia los objetivos de la Institución, como es proteger y auxiliar al ciudadano, fortaleciéndola.

Sumado, a que su estructura y diversificación consolidada, no sólo sirve para alianzas que generan redes sociales ya establecidas, sino también es facilitador de conexión entre comunidades e individuos alejados entre sí (Álvarez & Berni, 2001). Sin olvidar que, la cohesión y la confianza generada en ellas, facilitan que el conocimiento se difunda interna y externamente siendo un intangible valorado en la economía (Nonaka & Takeuchi, 2021), haciéndola más competitiva.

En consonancia a lo anteriormente expuesto, queda verificada nuestra última hipótesis (H6), finalizando con ella, nuestro objetivo de investigación.

H6: La economía social revierte en la Institución.

5. CONCLUSIONES

Una característica definitoria de nuestro tiempo es, cómo las empresas gestionan el capital social. La Institución responde al interrogante planteado por la nueva perspectiva económica dónde las organizaciones reflexionan sobre cuál es su aportación de valor para la sociedad (Retolaza & Alzola, 2021). Al analizarlo a través del CI de la Institución de la Guardia Civil, perteneciente al sector público y eminentemente social, exponemos que así como, los capitales no crean valor por sí solos tampoco lo hacen las inversiones por si solas en ellos. Serán las capacidades generadas por las empresas en la gestión de esos intangibles, las que conseguirán crecimiento económico (Hazan et al., 2021), a través de los servicios.

La Institución, al ejercer su actividad de seguridad y protección al ciudadano, va más allá creando mejoras en la vida de las personas y/o en la sociedad en su conjunto. Según muestran los datos, se debe al conocimiento, relaciones, cultura organizacional, experiencia y una participación activa de las personas que la componen. Deducimos, a través de los resultados obtenidos en la investigación llevada a cabo que, cumple uno de los objetivos marcados en el informe de la Alianza para la Inclusión Económica del Banco Mundial (2024), al poder ser evaluados sus programas sociales basados en evidencias claves.

ORCID: Https://orcid.org/0009-0000-2569-3710

Sus acciones presentan un modelo integrador llegando directamente a los más necesitados, generando cohesión social a través de la estructura institucional y su diversificación. Ya que dispone de una sólida estructura necesaria para la colaboración con otras organizaciones no gubernamentales, comunitarias y del sector privado (García-Flores & Palma, 2019) limando las limitaciones de capacidad.

El carácter benemérito de la Institución accionado por su personal, es valor social, quedando definido en este trabajo al mostrar el impacto positivo que tienen sus acciones en la sociedad. Al mostrarlo como un actor activo, abrimos una brecha en el estereotipo de la seguridad al ir más allá con sus acciones sociales, protección del medioambiente y biodiversidad. En este caso hemos presentando un modelo integrador que cree que, la solidaridad y cooperación es necesaria, elimina barreras sociales, y transforma entornos difíciles. Estos activos son valiosos para la Institución siguiendo el criterio VRIN de Barney (1991) al ser difíciles de imitar, comprar o sustituir, proporcionando ventaja competitiva.

Pensamos que datos adecuados y herramientas de medición, son imprescindibles para realizar unas políticas acertadas sobre cualquier tipo de capital. Con ello, se permite obtener información y mostrar a todas las partes interesadas, la inversión realizada con los resultados obtenidos (García-Porras, 2025), bajo el prisma de la transparencia. En esta investigación, se han recopilado y analizado datos cuantitativos y cualitativos, continuando líneas de investigación abiertas basadas en evidencias sobre los diferentes ecosistemas que acoge a la economía social, cumplimentando uno de los objetivos de la estrategia industrial marcada por la UE (Carini et al., 2024).

Finalizamos, con las contribuciones y limitaciones encontradas en este estudio. Los resultados muestran, por una parte, que las instituciones pertenecientes al sector público, pueden implicarse con organizaciones no gubernamentales y privadas como agente de cambio necesario, impulsando la economía social. Por otra, contribuimos a la aplicación del estudio de la gestión del CI en una Institución perteneciente al sector público ya que el estudio del CI está más focalizado en el sector privado. Pensamos que es novedoso investigar el valor social en una Institución frecuentemente estudiada bajo la óptica jurídica u operativa.

Respecto a las limitaciones encontradas, debe mencionarse que al estar basados sus datos en documentos institucionales podría generar un sesgo de fuente única. En la misma línea, los índices de los elementos obtenidos del CI no han sido ponderados, lo que minimiza la importancia relativa que puedan tener para el grupo de expertos específicos en economía social. Se necesitaría más investigación en este campo para incrementar nuestro entendimiento en este tema. Debido a ello, una futura línea de investigación podría robustecer este estudio mediante el uso de opiniones de expertos y otras percepciones externas y el planteamiento del uso de índices ponderados.

REFERENCIAS BIBLIOGRÁFICAS

Alvarez, S. A., & Barney, J. B. (2001). How entrepreneurial firms can benefit from alliances with large partners. *Academy Of Mana*gement Perspectives, 15(1), 139-148. https://doi.org/10.5465/ame.2001.4251563

Aramburu, N., Sáenz, J. y Rivera, O. (2005). Gestión del Conocimiento: Aspectos metodológicos y empíricos. Documento de trabajo. San Sebastián, Universidad de Deusto ESTE.

Arteaga A. L., Ojeda, J. F., y Alvarez D. G. (2020). Trayectoria y estrategias de emprendimiento en mujeres. *aDResearch ESIC International Journal Of Communication Research*, 22(22), 176-195. https://doi.org/10.7263/adresic-022-10

Barney, J. (1991). Firm Resources and Sustained Competitive Advantage. Journal of Management, 17(1), 99-120. https://doi.org/10.1177/014920639101700108

Bellucci, M., Marzi, G., Orlando, B., & Ciampi, F. (2021). A review of emerging themes and future trends. *Journal of intellectual capital*, 22(4),744-767. https://doi.org/10.1108/JIC-10-2019-0239

Bini, L., Bellucci, M., & Giunta, F. (2017). Integrating sustainability in business model disclosure: Evidence from the UK mining industry. *Journal* o*f Cleaner Production*, 171, 1161-1170. https://doi.org/10.1016/j.jclepro.2017.09.282

Briñez M. E. (2021). Tecnología de información: ¿Herramienta potenciadora para gestionar el capital intelectual? *Revista de Ciencias Sociales 27*(1)*,* 180-192. https://dialnet.unirioja.es/servlet/articulo?codigo=7817690

Bontis, N. (2002). Intellectual capital disclosure in Canadian corporations. Journal of Human Resource Costing and Accounting, 7(1–2), 9–20.

Bueno E. J. y Merino C. (2007). El capital intelectual y la creación de empresas en la sociedad. *Encuentros multidisciplinares*, *(9)26*, 37-46. https://dialnet.unirioja.es/servlet/articulo?codigo=2324790

Bueno, E. J., Salmador, M. P. y Merino, C. (2008). Génesis, concepto y desarrollo del capital intelectual en la economía del conocimiento: Una reflexión sobre el Modelo Intellectus y sus aplicaciones. Estudios de Economía Aplicada, 26(2), 43-63. https://www.redalyc.org/pdf/301/30113187003.pdf

Burt, R. S. (2004). Brokerage and Closure: An Introduction to Social Capital.

http://ronaldsburt.com/research/files/B&C_Introduction.pdf

Cañibano L., Sánchez, P., García-Ayuso, M., y Chaminade, C. (2002). Proyecto MERITUM. Directrices para la gestión y difusión de información sobre intangibles (Informe de capital intelectual). Fundación Vodafone.

https://dialnet.unirioja.es/servlet/libro?codigo=448252

Carini, Ch., Galera, G., Tallarini, G., Chaves, A., Sak, B. & Schoenmaeckers, J., (2024). *Benchmarking the socio-economic performance of the EU Social Economy.* European Commission.

https://eismea.ec.europa.eu/news/study-benchmarking-socio-economic-performance-eu-social-economy-now-published-2024-09-19_en

Comisión Europea (CE, 2006). Reporting intellectual capital to augment research, development *and innovation in SMEs: report to the Commission of the High Level* Expert Group on RICARDIS (Comisión Europea. Dirección General de Investigación ed.). Luxemburgo: Oficina de Publicaciones Oficiales de las Comunidades Europeas.

https://op.europa.eu/es/publication-detail/-/publication/60cbf27c-5552-429f-a077-44135a97cc27/language-en

Chen, Y. S. (2008). The positive effect of green intellectual capital on competitive advantages of firms. *Journal of Business Ethics*, (77)3, 271–286. https://doi.org/10.1007/s10551-006-9349-1

Chen, H., Shih A. & S. Y. Yang, (2009). The Role of Intellectual Capital in Knowledge Transfer. IEEE Transactions on Engineering Management, (56)3, 402-411.

https://ieeexplore.ieee.org/abstract/document/5072284

Codina, L., Morales-Vargas, A., Rodríguez-Martínez, R. Y Pérez-Montoro, M. (2020). Uso de Scopus y Web of Science para investigar y evaluar en comunicación social. Análisis comparativo y caracterización. Index.ComunicacióN/Index Comunicación, 10(3), 235-261. https://doi.org/10.33732/ixc/10/03usodes.

Davenport, T. y Prusak, L. (2001). Conocimiento en acción. Buenos Aires: Prentice Hall. Argentina.

De Castro, G. y García-Muiña, F. E (2003). Hacia una visión integradora del capital intelectual de las organizaciones. Concepto y componentes. Boletín Económico de ICE, Información Comercial Española, 2756, 7-16. https://dialnet.unirioja.es/servlet/articulo?codigo=303756

Delgado, M., Navas, J.E., Martín. G. & López, P. (2008). La innovación tecnológica desde el marco del capital intelectual. Cuaderno de Trabajo 04/2008. Universidad Complutense Madrid.

Demartini, C., & Trucco, S. (2016). Does Intellectual Capital Disclosure Matter for Audit Risk? Evidence from the UK and Italy. Sustainability, 8(9), 867. https://doi.org/10.3390/su8090867

Díaz B. F. y Lejarriaga G. (2019). Presentación del monográfico: Emprendimiento social y empleabilidad. REVESCO. Revista de Estudios Cooperativos, 129, 9-15. https://doi.org/10.5209/REVE.62962

Diaz-Foncea M., Marcuello S. y Monreal G. (2016). Economía social y economía colaborativa: Encaje y potencialidades. Economía industrial, 402, 27-35 https://www.mintur.gob.es/Publicaciones/Publicacionesperiodicas/EconomiaIndustrial/RevistaEconomiaIndustrial/402/D%C3%8DAZ%20FONCEA,%20MARCUELLO%20Y%20MONREAL.pdf

Dumay, J., Bernardi, C., Guthrie, J., & Demartini, P. (2016). Integrated reporting: A structured literature review. *Accounting Forum*, 40(3), 166-185. https://doi.org/10.1016/j.accfor.2016.06.001

Edvinsson, L. y Malone, M.S. (1999). El capital Intelectual. Barcelona: Gestión, 2000.

Fernández , D. J. Guevara, G. D. , Dávila T. L. y Cruz, J. J. (2022). Capital intelectual como factor del desempeño organizacional en las Micro y Pequeñas Empresas. Revista de Investigación en Comunicación y Desarrollo, 13(1), 63-73. https://doi.org/10.33595/2226-1478.13.1.595

Fernández-Solís, C., González-Ramírez, M. R., y Gascó-Gascó, J. (2025). La intención de adopción de la analítica de recursos humanos y su impacto en el desempeño organizacional: una aproximación teórica. *INNOVA Research Journal*, 10(1), 93-111. https://doi.org/10.33890/innova.v10.n1.2025.2706

Garanina T., Hussinki H., & Dumay J. (2021). Accounting for intangibles and intellectual capital: A literature review from 2000 to 2020, *Accounting & Finance*, forthcoming. https://doi.org/10.1111/acfi.12751

García-Flores, V. y Palma Martos, L. P. (2019). Innovación social: Factores claves para su desarrollo en los territorios. CIRIEC-España Revista de Economía Pública Social y Cooperativa, 97, 245-278. https://doi.org/10.7203/ciriec-e.97.14148

García-Flores, V. y Palma Martos, L. P. (2020). Entidades del tercer sector e innovación social. Elementos caracterizadores y factores de éxito. REVESCO Revista de Estudios Cooperativos, 136, e71861. https://doi.org/10.5209/reve.71861

García-Porras, B. (2025). Presentación del informe estadístico CIRIEC, Euricse y Spatial Foresight. Evaluación comparativa de los resultados socioeconómicos de la Economía Social de la UE. https://ciriec.es/noticias/el-nuevo-informe-de-euricse-ciriec-internacional-y-spatial-foresight-impulsado-por-la-comision-europea-cifra-en-115-millones-las-personas-empleadas-en-la-economia-social-en-la-ue/

Grant, R. M. (1996). Toward a Knowledge-Based Theory of the Firm. Strategic Management Journal, 17, 109-122. https://doi.org/10.1002/smj.4250171110

Guthrie, J. & Abeysekera, I. (2006). Content analysis of social, environmental reporting: What is new?, Journal of Human Resource Costing & Accounting, 10(2), 114-126. https://doi.org/10.1108/14013380610703120

Hazan, E., Smit, S., Woetzel J., Cvetanovski, B., Krishnan, M., Gregg, B., Perrey J. & Hjartar, K. (2021). Getting tangible about intangible. The future of grow and productivity? Mckinsey Global Institute. https://doaj.org/article/faecfbdaace64e669c135ccadc104776

Haarhaus, T. & Liening, A. (2020). Building dynamic capabilities to cope with environmental uncertainty: The role of strategic foresight. T*echnological Forecasting and Social Change*, 155. https://doi.org/10.1016/j.techfore.2020.120033

Jeffrey, S., Rosenberg, S. & McCabe, B. (2019). Corporate social responsibility behaviors and corporate reputation. *Social Responsibility Journal,* 15(3), 395-408. https://doi.org/10.1108/SRJ-10.11-2017-0255

Johnson, W.H.A. (1999). An integrative taxonomy of intellectual capital: Measuring the stock and flow of intellectual capital components in the firm. International Journal of Technology Management, 18(5-8), 562-575.

Lev, B. (2001). *Intangibles: Management, Measurement, and Reporting*. Washington DC: Brookings Institution Press. http://www.jstor.org/stable/10.7864/j.ctvcj2rf2

Li, X., Nosheen, S., Haq, N. U., & Gao, X. (2020). Value creation during fourth industrial revolution: Use of intellectual capital by most innovative companies of the world. *Technological Forecasting And Social Change*, 163, 120479. https://doi.org/10.1016/j.techfore.2020.120479

López P., Martín de Castro, G., y Navas, J.E. (2004). Una aproximación a las relaciones entre elementos del capital intelectual de las organizaciones. Boletín Económico de ICE (2817). https://www.revistasice.com/index.php/BICE/article/view/3626/3626

Maqbool, S., Rasool, H., & Ahmad, S. (2018). Corporate Social Responsibility and Financial Performance: An Empirical Analysis of Indian Banks. Future Business Journal, 4(1), 2314-7210. https://doi.org/10.2139/j.fbj.2017.12.002

Magau, M. D., Roodt, G., & van Zyl, G. (2021). A measurement scale for assessing intellectual capital disclosure. *Journal of HumanResource Management, 19*, 1–14. https://doi.org/10.4102/sajhrm.v19i0.1645

Merino C., Alonso, M., González, N., y Plaz, R. (2018). Gestión del conocimiento en organizaciones del sector nuclear. Universidad Nacional de Educación a Distancia (UNED).

Ministerio del Interior (GC, 2023). Memoria de Sostenibilidad Guardia Civil 2023. https://www.interior.gob.es/opencms/pdf/archivos-y-documentacion/documentacion-y-publicaciones/publicaciones-descargables/publicaciones-periodicas/memoria-RSC-Sostenibilidad-de-la-Guardia-Civil/Memoria-sostenibilidad-GC_126230302_pdfWEB.pdf

Ministerio Trabajo y Economía Social (MITES). Informe de evolución y Tendencias en el ámbito de la Economía Social (2023). Confederación Empresarial Española de la Economía Social (CEPES). https://www.fundae.es/docs/default-source/publicaciones-y-evaluaciones/publicaciones-econom%C3%ADa-social/1-1-evoluci%C3%B3n-y-tendencias-de-la-ec-social_2023.pdf

Mohdzaini, H. (2021). Technology and the future of work: How artificial intelligence (AI) robots and automation are shaping the world of work, m the ethical considerations and the role of people professionals. CIPD. https://www.cipd.org/uk/knowledge/factsheets/emerging-future-work-factsheet/

Moreiro J. A., Morato J., Sánchez S. y Rodríguez B. A., (2006). Categorización de los conceptos en el análisis de contenido: su señalamiento desde la Retórica clásica hasta los Topic Maps. *Investig*ación Bibliotecnológica: Archivonomía, bibliotecología e información, *20*(40). https://doi.org/10.22201/iibi.0187358xp.2006.40.4097

Navarro González A. y Medina Jiménez, A., (2024). Relación del Capital intelectual con el capital humano, estructural y relacional. Trascender Contabilidad y Gestión, 9(26), 100-127. https://doi.org/10.36791/tcg.v9i26.260

Nonaka, I. & Takeuchi, H. (1995). *The knowledge creating company*. New York: Oxford University Press.

Nonaka, I. & Konno, N. (1998). The Concept of Ba: Building a Foundation for Knowledge Creation. California Management Review, 40, 40-54. https://doi.org/10.2307/41165942

Nonaka, I., & Takeuchi, H. (2021). Humanizing strategy. Long Range Planning, 54(4), 102070. https://doi.org/10.1016/j.lrp.2021.102070

Oliveira, M., Curado, C., Balle, A. R., & Kianto, A. (2020). Knowledge sharing, intellectual capital and organizational results in SMES: are they related? Journal of Intellectual Capital, 21(6), pp. 893–911. https://doi.org/10.1108/JIC-04-2019-0077

Organisation for Economic Co-operation and Development (2006). Creating Value from Intellectual Assets. Meeting of the OECD Council at Ministerial Level.

Pedreño, J., (2024). The social economy and The EU 2024-2029 Objectives. Europe Social Economy. https://www.socialeconomy.eu.org/2024/10/22/great-sucess-of-the-event-the-social-economy-and-the-eu-2024-2029-objectives/

Petty, R., & Guthrie, J. (2000). Intellectual capital literature review. *Journal Of Intellectual* Capital, 1(2), 155-176. https://doi.org/10.1108/14691930010348731

Porter, M. (1996). What is strategy? *Harvard Business Review 74*(6), 61–78. https://iqfystage.blob.core.windows.net/files/CUE8taE5QUKZf8ujfYlS_Reading+1.4.pdf

Retolaza, J. y Alzola, M. (2021). Aplicando el valor social en las organizaciones. Boletín de Estudios Económicos, 76(232), 19-22. https://doi.org/10.18543/bee.2383

Rideg, András, Szerb, László, & Róza Varga, Anna. (2023). The role of intellectual capital on innovation: Evidence from Hungarian SMEs. Tec Empresarial, 17(2), 1-19. https://www.researchgate.net/publication/370608181_The_role_of_intellectual_capital_on_innovation_Evidence_from_Hungarian_SMEs

Roos, J. (2001). Capital intelectual: el valor intangible de la empresa. Barcelona: Paidós.

Sánchez-Espada J., Martín S., Bel P. y Lejarriaga G. (2018). Educación y formación en emprendimiento social: características y creación de valor social sostenible en proyectos de emprendimiento social. REVESCO. Revista de Estudios Cooperativos, 129, 16-38. http://dx.doi.org/10.5209/REVE.62492

Secundo, G., Ndou, V., Del Vecchio, P., & De Pascale, G. (2020). Sustainable development, intellectual capital and technology policies: A structured literature review and future research agenda. Technological Forecasting And Social https://doi.org/10.1016/j.techfore.2020.119917

Stratone, M. (2023). A Bibliometric Analysis of the Role of the Intellectual Capital in the Organizational Agility and Performance. Proceedings Of The International Conference On Business Excellence, 17(1), 1275-1285. https://doi.org/10.2478/picbe-2023-011

Steward, T. (1997). La nueva riqueza de las organizaciones: el capital intelectual Buenos Aires: Ediciones Granica S.A.

Suciu, M., & Năsulea, D. (2018). Intellectual Capital and Creative Economy as Key Drivers for Competitiveness Towards a Smart and Sustainable Development: Challenges and Opportunities for Cultural and Creative Communities. En: Intellectual Capital Management as a Driver of Sustainability. https://doi.org/10.1007/978-3-319-79051-0_5

Sumedrea, S. (2013). Intellectual Capital and Firm Performance: A Dynamic Relationship in Crisis Time. *Procedia Economics And Finance*, *6*, 137-144. https://www.sciencedirect.com/science/article/pii/S2212567113001251?via%3Dihub

Teece, D.J., Pisano, G. & Shuen, A. (1997). Dynamic capabilities and strategic management. Strategic Management Journal, 18(7), 509-533

Thum-Thysen, A., Voigt, P., & Weiss, C. (2021). Refections on Complementarities in Capital Formation & Production: Tangible & Intangible Assets across Europe. Euopean Commission/EuropeanEconomy[online]https://economy-finance.ec.europa.eu/document/download/3ddd17a1-0d58-4614-a363-90a9e6a12e9c_en?filename=dp152_en.pdf

Wang, C.N., Chang, Y.L., Huang, Q.H. & Wang, C.H. (2011). Assessment on intellectual capital management for Taiwanese pharmaceutical industry: using GRA and MPI. African Journal of Business Management 5(7), 2950-2958

https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=78a492920f297eb118e7972ef4ad52ce99ec2355

Word Bank Group (2024). Annual Report 2024. https://openknowledge.worldbank.org/bitstreams/91a20260-c3c4-4ed7-a488-d7dd8d419c8a/download

Xu, J., & Wang, B. (2018). Intellectual Capital, Financial Performance and Companies' Sustainable Growth: Evidence from the Korean Manufacturing Industry. Sustainability, 10(12), 4651. https://doi.org/10.3390/su10124651

Zheng S., Zhang W., Wu X. & Du J. Know ledge-based Dynamic capabilities and innovation in networked environments. Journal of Knowledge Management 15(6), 1035-1051.

ORCID: Https://orcid.org/0009-0000-2569-3710

Anexo I

Tablas 4-6: Unidades muestrales y definición dimensiones del CI en la Institución

ELEMENTOS DIMENSIÓN CAPITAL HUMANO		
Códigos	Unidad Muestral	Definición
CHIDENTIDAD	Pertenencia y compromiso.	Identificación de las personas como guardias civiles dentro de la Institución.
CHMOTIVACION	Automotivación	Los impulsos conscientes que hacen a los guardias civiles conseguir desempeñar el servicio con excelencia.
CHSATISFACCION	Satisfacción	Forma de participar en el desempeño de su trabajo y comportamientos de los guardias civiles en la Institución. Evaluación desempeño.
CHCREATIVO	Creatividad. Cultura innovadora	Creación de ideas nuevas y aplicables al desempeño del servicio. La forma de impulsar los pensamientos nuevos, ideas y actitudes por la Institución para generar nuevas formas de actuación o una mejora de las existentes.
CHEDUCACION	Educación reglada.	Conocimientos explícitos que posee en general los guardias civiles.
CHESPECIALIDAD	Formación especializada.	Conocimientos específicos de una especialidad concreta o trabajo técnico en la Institución
CHUNIVERSITARIO	Inversión en formación Universitaria.	Centro Universitario Guardia Civil (CUGC).
CHFORMACION	Formación interna.	Conocimientos adquiridos mediante programas, jornadas, talleres, y todos los cursos de formación que comprenden la capacitación y promoción interna en las Academias y en el Centro Universitario de la GC.
CHEXPERIENCIA	Experiencia.	Conocimientos adquiridos mediante el desempeño realizado en la Institución.
CHDESARROLLO	Desarrollo personal.	Conocimientos adquiridos informalmente en la Institución. Personas que promocionan. Promoción interna.
CHAPRENDIZAJE	Aprendizaje	Adquisición de nuevos conocimientos. Jornadas PATIO Y SIO.
CHCIVIL	Colaboración, personal civil.	Capacidad de trabajar con otras personas: compañeros, personal administraciones públicas. Personal civil funcionariado.
CHCONCILIA	Conciliación vida familiar profesional	Favorecer el equilibrio entre la vida familiar y la laboral a los guardias civiles. Compatibilizar la vida profesional y familiar.
CHLIDERAZGO	Liderazgo.	Guiar y mover a los compañeros hacia el desempeño de un servicio con excelencia y otras personas relacionadas con el servicio.

ELEMENTOS DIMENSIÓN CAPITAL ESTRUCTURAL

Códigos	Unidad Muestral	Definición
CECULTURA	Homogeneidad cultural.	Aceptación de los valores de la Guardia Civil.
CECLIMA	Clima social-laboral.	Ambiente generado en la unidad, departamento o equipo de trabajo. Índice de clima social.
CEIGUALDAD	Sensibilidad género. Igualdad.	Introducción de la perspectiva de género en la Institución. Igualdad de condiciones entre hombres y mujeres acceso mismo puesto bajo las mismas condiciones e iguales requisitos
CESTRUCTRURA	Diseño organizativo. Plantilla. Delimitación competencias	Estructura de la Institución que establece las relaciones laborales. Distribución. Competencias funcionales.
CEDESARROLLO	Desarrollo organizativo.	Acontecimientos que propician adaptación a las situaciones actuales. Regulación de Jornadas y horarios en general.
CERUTINAS	Pautas organizativas. Procedimientos establecidos y sistemas.	Procedimientos y rutinas establecidos o nuevas competencias para mejorar la Institución. Mejora de las funciones a desempeñar por los guardias civiles, mejorando su calidad profesional y aumentando su motivación.
CERELACIONINT	Explicación de la estrategia a su personal.	Procesos dirigidos a explicar a los componentes de la Institución su Estrategia, visión, misión e innovación. Introducción de algo nuevo o modificación de lo anterior que provoque un mejor desempeño en el servicio.
CECRIMINAL	Actuaciones, denuncias e infracciones administrativas.	Procesos dirigidos a explicar, numerar y contextualizar las detenciones, denuncias e infracciones administrativas.
CEPROVEEDORES	Contratación proveedores.	Conjunto de procesos de proveedores, alineados a los valores de la Institución. Contratación pública socialmente responsable (CPSR).Orientado a los riesgos laborales, reciclaje y medio ambiente.
CEINVERSIONIDi	Inversión I+ D+ i. Dominios de sus sedes electrónicas.	Inversión económica en investigación y desarrollo. Gastos elaborados por su funcionamiento al desarrollar acciones innovativas, conferidas como espacios virtuales de uso exclusivo por la Institución. Dominios internet.
CEPERSONALIDi	Personal I+D+i.	Plantilla de plena dedicación a investigación y desarrollo.
CEPROYECTOSIDi	Proyectos I+D+i. Programa Marco UE. Programa Horizonte 2020.	Trabajos realizados relacionados con la innovación y el desarrollo. Proyectos generados en concordancia con el proceso innovativo con otras organizaciones o de forma independiente.
CEINFRAESTRUCTURA	Infraestructuras y material.	Mantenimiento de las instalaciones. Inversión en instalaciones e infraestructuras.
CEEQUIPOPOLICIAL	Equipamiento policial. Dotación tecnologías de producción.	Productos y herramientas adecuadas a las necesidades particulares de la Institución. Conjunto de equipos tecnológicos necesarios para el cumplimiento de un servicio.
CEINNGEST	Innovación de gestión. Innovación de modelo de Institución.	Herramientas nuevas y procedimientos compartidos en la Institución que impulsan la innovación. Transformación digital.
CECOMUNICACIONGC	Comunicación interna Relaciones asociaciones. Consejo.	Sistemas informáticos, telecomunicaciones útiles funcionamiento de la Institución. Facilidad y buena actitud en la transmisión de los conocimientos e información para la ejecución de un servicio con las personas adecuadas para ello. Atención al guardia civil.
CEMARCA	Marcas registradas. Imagen de la GC	Marca, logo y emblemas en la Institución. Referencia a los uniformes.
CELICENCIAS	Licencias forenses, subscriptores.	Procesos por el que se comparte una parte de los procesos y conocimientos de la Institución. Convenios con otras administraciones y universidades.
CESECRETO	Protección de datos.	Todos los considerados por la Institución como tales. Protección de datos (ciudadanos).
CEPATENTES	Información patentes.	Base de datos registren cantidad y uso de patentes empleadas por la Institución.
CETECNOEXT	Conocimiento actividad tecnológica competencia.	Bases de datos e información disponible sobre los avances en I+D de los competidores.
CETECNONEW	Información sobre líneas investigación y tecnología emergente.	Bases de datos de información sobre tecnología emergente que afecte a la Institución. Conocimiento posibles asociaciones con empresas para I+D.
CETECLIC	Localización tecnología sobre la que buscar licencias	Fuentes de datos sobre tecnologías útiles para ser desarrolladas en la Institución.
CEFLEXIBILIDAD	Flexibilidad y adaptabilidad.	Comportamiento favorable hacia el cambio por las situaciones derivadas del servicio o de la Institución.
CETALENTOS.	Antigüedad y fidelización de los guardias civiles.	Permanencia de los empleados basada en políticas de retención y atracción de guardias civiles que aportan valor a la Institución. Situaciones.

ORCID: Https://orcid.org/0009-0000-2569-3710

ELEMENTOS DIMENSIÓN CAPITAL RELACIONAL

Códigos	Unidad Muestral	Definición
CRCIU	Base ciudadanos.	Ciudadanos en general.
CRLEALCIU	Lealtad ciudadanos.	Grado de fidelidad que procesan los ciudadanos a la Institución. Primera opción en seguridad.
CRSATISFACCION	Satisfacción ciudadanos. Seguridad pública.	Grado de eficacia que el ciudadano percibe en la cumplimentación de un servicio y en general con la Institución. Felicitaciones atención al ciudadano.
CRQUEJAS	Quejas, reclamaciones y sugerencias ciudadanos.	Quejas recibidas por la prestación de un servicio y sugerencias. Atención a la ciudadanía. Oficina de Información y Atención al Ciudadano(OIAC). Puntos de Atención Especializada (PAEs).
CRPROTCIU	Procesos relación ciudadanos. Protocolos ciudadanos.	Protocolos de actuación y comportamiento con los ciudadanos. Turismo seguro. Trata de seres humanos (TSH). Mayores seguros. VdG. Menores. Víctimas de terrorismo.
CRESTADO	Relaciones Estado y UE. Accionistas e inversiones institucionales.	Grado de inversiones; recursos disponibles; presupuestos.
CRIADMINISTRACION	Relaciones Institución mercado. Relaciones con otros grupos de interés Administración.	Relaciones con otros grupos de interés de la Institución. Administración general ACCEDA; Firma digital. Partidos políticos. Firma convenios administraciones.
CRCAPITALEXTERIOR	Relaciones participación empresarial.	Capital de la Institución en otras entidades.
CRALIANZAS	Base aliados.	Alianzas con otras instituciones dentro de su área de seguridad. Relacionados con la creación de conocimiento, y su transferencia impulsando la innovación.
CRALIANZASESTABLES	Solidez alianzas. Servicios conjuntos. Estabilidad alianzas y formalización.	Formas establecidas de cooperación con policías misma área de seguridad. Innovación internacional. Nuevas formas en otros países que contribuyan al desarrollo o diversificación de la Institución o sus competencias. Misiones encomendadas por el Ministerio de Defensa.
CRALIANZASBENEFICIO	Beneficio alianzas. Resultados obtenidos alianzas.	Generación de beneficios de las alianzas establecidas. Ayuntamientos Seguridad Ciudadana y Seguridad Vial. Protección civil.
CRCONCOMPETENCIA	Conocimiento competidores.	Conocimiento otras policías en la compartición de las competencias de seguridad.
CRPRIVADA	Relaciones seguridad privada.	Grado beneficios obtenido relaciones con otros grupos de interés. Seguridad privada.
CRCERTICAL	Certificaciones y sistemas calidad.	Certificados de calidad otorgados a la Institución. Premios (SEPRONA); Igualdad.
CRREDES	Portal guardia civil exterior. Información divulgada redes.	Canales de comunicación en la Institución basado en la tecnología. Notas de prensa e información comparte Institución en Redes Sociales. Información pública.
CRADMINISTRACION	Colaboración Adm. Públicas. Cooperación para el desarrollo.	Cooperación con otras administraciones nacionales e internacionales de la Institución. Ministerios. Compras públicas innovadoras firma de Convenios con otras administraciones.
CRMEDIOS	Relaciones medios comunicación convencionales.	Exposición de la institución medios de comunicación. TVE; radio; periódicos. Medios más convencionales.
CRDEFENSAMBIENTE	Relaciones instituciones defensa medioambiental.	Grado de efectividad con otros grupos dedicados a la defensa del medioambiente.
CRVERDE	Códigos y certificaciones medio ambientales.	Procedimientos y protocolos establecidos interiorizados por la Institución en la defensa del medioambiente.
CRMERCADO	Relaciones instituciones mercado trabajo.	Relaciones institución con el mercado laboral. Contribución al tejido empresarial Oferta empleo público (OEP).
CRCODIGOCON	Código de conducta.	Nuestro código es normativo. Normas explícitas establecidas de comportamiento recogidas en el Reglamento. Código Penal Militar.
CRACSOCIAL	Acción social al ciudadano. Preocupaciones sociales	Espíritu Benemérito. Comportamiento adecuado y correcto del personal especialmente con los ciudadanos en el desempeño del servicio. Responsabilidad con la sociedad, desarrollo económico, solidaridad e integración social.
CRBUENGOBIERNO	Dirigidos a los ciudadanos. Buen gobierno.	Procesos dirigidos a la catalogación de los ciudadanos, sus riesgos y necesidades. Código buen gobierno de la AGE. Difusión de buenas prácticas. Transparencia, responsabilidad y eficacia con todos los grupos de interés. Compromiso adquirido voluntario por la Institución como forma de rendir cuentas a la sociedad a la que sirve.

Anexo II

Ejemplos de cálculo de un índice de un elemento, perteneciente a cada categoría.

Categoría Capital Humano

Elemento: *CHEducación*.

$$\text{I CHEducación } = 1/14 \sum_{i=1}^{14} j = \text{I CHEducación } \textit{cuanti} + \text{I CHEducación } \textit{cualit} + \text{I CHEducación } \textit{gráfico}$$

Categoría Capital Estructural

Elemento: *CERutinas*.

$$\text{I CERutinas } = 1/25 \sum_{i=1.}^{25} j = \text{I CERutinas } \textit{cuanti} + \text{I CERutinas } \textit{cualit} + \text{I CERutinas } \textit{gráfico}$$

Categoría Capital Relacional

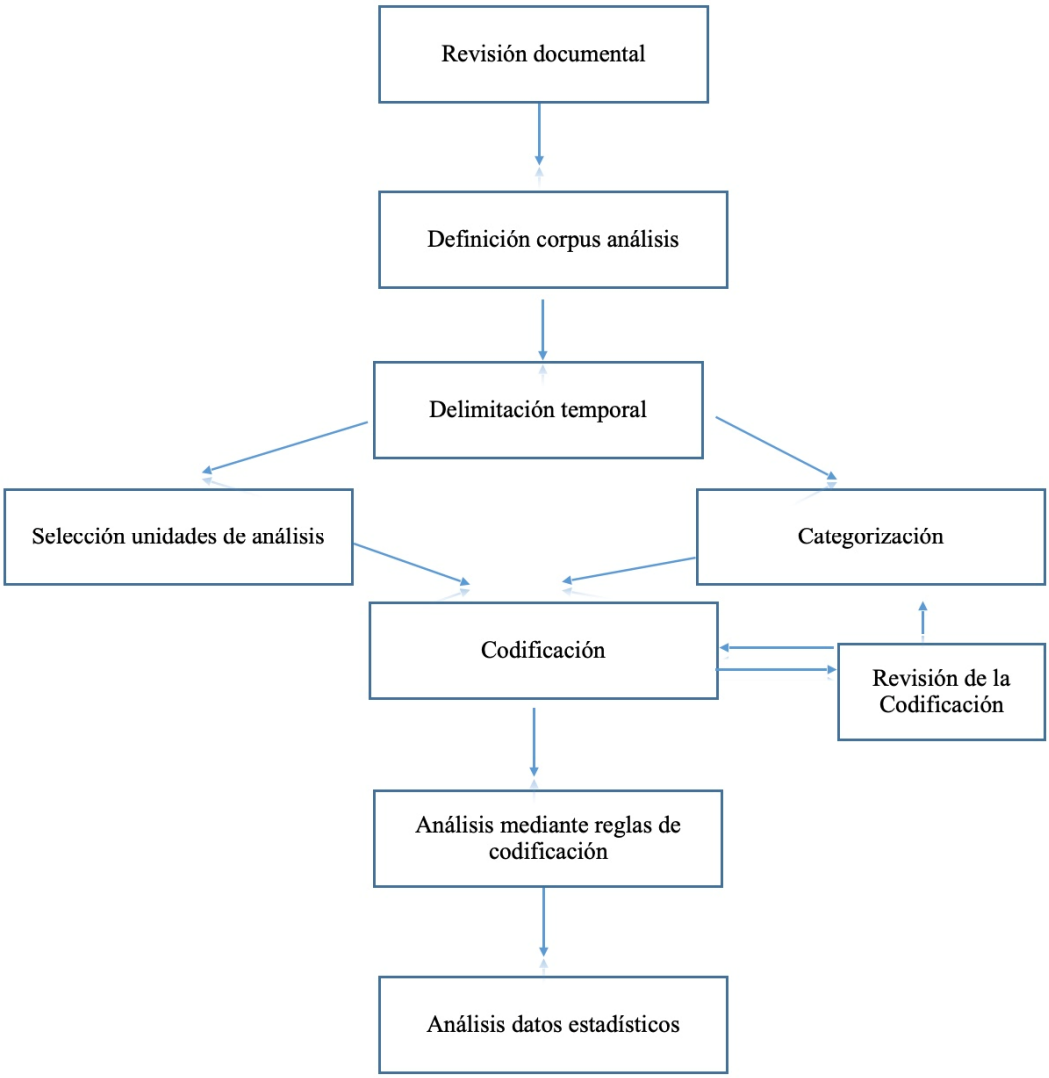
Elemento: CRLealciu.

$$\text{I CRLealciu } = 1/23 \sum_{i=1.}^{23} j = \text{I CRLealciu } \textit{cuanti} + \text{I CRLealciu } \textit{cualit} + \text{I CRLealciu } \textit{gráfico}$$

ORCID: Https://orcid.org/0009-0000-2569-3710

Anexo III

Fases desarrolladas en el análisis de contenido



Revista Científica del Centro Universitario de la Guardia Civil
Revista Lógos Guardia Civil

III.- RESEÑAS DE JURISPRUDENCIA

Revista Científica del Centro Universitario de la Guardia Civil
Revista Lógos Guardia Civil

Reseña de jurisprudencia

RESEÑA DE JURISPRUDENCIA SALA 2ª TRIBUNAL SUPREMO

Javier Ignacio Reyes López
Magistrado del Juzgado de Instrucción número 46 de Madrid
Diploma de Estudios Avanzados (DEA)
ji.reyes@poderjudicial.es

Recibido 06/06/2025
Aceptado 06/06/2025
Publicado 27/06/2025

Cita recomendada: Reyes, J. I. (2025). Reseña de jurisprudencia Sala 2ª Tribunal Supremo. *Revista Logos Guardia Civil*, 3(2), p.p. 295-320.

Licencia: Este artículo se publica bajo la licencia Creative Commons Atribución-NoComercial-SinDerivadas 4.0 Internacional (CC BY-NC-ND 4.0)
Depósito Legal: M-3619-2023
NIPO en línea: 126-23-019-8
ISSN en línea: 2952-394X

RESEÑA JURISPRUDENCIA SALA 2ª TRIBUNAL SUPREMO

Sumario: 1.- STS 350/2025, de 10 de abril. Concepto de interesado en un registro domiciliario. 2.- STS 358/2025, de 10 de abril de 2025. Noticia criminal traslada a España por una autoridad judicial extranjera y continuación de la investigación en nuestro país con nuevas investigaciones. 3.- STS 324/2025, de 07 de abril de 2025. Conservación de datos de las comunicaciones. 4.- STS 294/2025, de 28 de marzo de 2025. Principio de insignificancia y de toxicidad en los delitos contra la salud pública. 5.- SAN 8/2025, Penal Sección 3ª, de 2 de abril de 2025. Delito de estragos con fines terroristas. 6.-STS 308/2025, de 2 de abril de 2025. Investigación policial en España que surge a partir del conocimiento de una OEDE dictada por las autoridades judiciales de otro país por otro hecho delictivo. Presencia de los detenidos en un registro domiciliario. 7.- STS 295/2025, de 28 de marzo de 2025. Delito de acoso, "stalking". 8.- STS 284/2025, de 27 de marzo. Abuso sexual sobre persona de 17 años con inteligencia límite. Daño moral.

1.- STS 350/2025, de 10 de abril. Concepto de interesado en un registro domiciliario[1].

Antecedentes de hecho.

El Juzgado de Instrucción nº 5 de Marbella incoó procedimiento abreviado nº 104/2018 por un presunto delito contra la salud pública contra Noelia, entre otros, que una vez concluido remitió para su enjuiciamiento a la Sección 1ª de la Audiencia Provincial de Málaga. Incoado el procedimiento abreviado nº 1004/2019 con fecha 17 de mayo de 2021, dictó la sentencia nº 233/2021 en la que declaraba como probado que, "…Apreciando en conciencia la prueba practicada, expresa y terminantemente se declara probado que por parte del Grupo de Delincuencia Urbana de la Comisaria del CNP Marbella, se realizó un dispositivo de vigilancia, al objeto de detectar la venta de sustancias en la zona xx de Marbella, que se encuentra situada entre el Polígono la Ermita y el Bulevar de la Avenida José Manuel Valles y junto a un centro escolar, punto frecuente y muy conocido por su conflictividad y por ser un punto de venta y consumo de drogas. Se tuvo conocimiento de la existencia del clan de los "Chatos" dedicado a la venta de sustancias estupefacientes a través de inmuebles radicados en dicha barriada marginal, ya que tenían noticias de sus moradores pudieran estar dedicándose a la venta de sustancias estupefacientes, al existir un diario trasiego de personas que realizaban visitas de corta duración. Fruto de la vigilancia, observación exhaustiva, la interceptación y aprehensión sucesiva, mediante actas de droga procedentes de personas que habían acudido específicamente a comprar en los domicilios investigados, se recogen las siguientes actas…y posteriormente, a partir de la petición policial, por el Juzgado de Instrucción n° 5 de Marbella se dictó auto de fecha 4 de junio de 2018 autorizando la entrada y registro, entre otros, en los varios domicilios en los que fueron aprehendidas sustancias estupefacientes y detenidos los investigados…"

[1] STS 350/2025, Penal sección 1 del 10 de abril. Publicada en la página web del Centro de Documentación Judicial, CENDOJ, (ROJ: STS 1701/2025 - ECLI:ES:TS:2025:1701), recurso nº 7569/2022. Ponente, Excmo. Sr, D. Eduardo de Porres Ortiz de Urbina.

Fundamentos jurídicos.

Se recurre en casación ante el Tribunal Supremo la sentencia número 197/2022, de 14 de julio de 2022, dictada por la Sala de lo Civil y Penal del Tribunal Superior de Justicia de Andalucía, Ceuta y Melilla, que desestimó el recurso de apelación interpuesto contra la sentencia número 233/2021, de 17/05/2021, de la Sección 1ª de la Audiencia Provincial de Málaga, condenatoria por un delito contra la salud pública. De las cuatro personas condenadas sólo ha interpuesto recurso una de ellas.

En el primer motivo del recurso se reprocha a la sentencia impugnada la vulneración del derecho a la intimidad domiciliara del artículo 18.2 CE y el derecho a un proceso con todas las garantías reconocido en el artículo 24.2 también del texto constitucional.

Alega que estaba en situación de detención cuando se practicaron los registros domiciliarios y sólo pudo estar presente en uno de ellos (el del domicilio del que salía cuando fue detenida) y no en los otros domicilios, respecto de los que se le atribuía una relación delictual.

Entiende la defensa que la presencia del interesado es requisito inexcusable del registro domiciliario conforme al art. 569 LECrim, siendo nulas las injerencias domiciliarias que no cumplan con esta exigencia cuando el interesado esté detenido y no exista otra razón que lo haga imposible, por lo que no es hábil como prueba de cargo, y tampoco son valorables como prueba de cargo las declaraciones de los agentes policiales que hubieran intervenido en ellas.

Considera que, en el presente caso, la nulidad del registro conduce a la imposibilidad de afirmar legalmente el hallazgo de la sustancia y objetos de cuya detentación deviene la condena por los delitos contra la salud pública y tenencia ilícita de armas y que dicha incautación no puede ser sanada por medio de la declaración de los agentes presentes en el registro pues sus respectivos testimonios están ligados de manera directa a la ilícita diligencia.

Esta cuestión fue planteada en el previo recurso de apelación y los argumentos de su desestimación los hacemos nuestros.

En este procedimiento se practicaron siete registros simultáneos y en cinco de ellos se llevó a cabo la diligencia en presencia de las personas interesadas en cada uno de los inmuebles, salvo en dos ellos en que no se encontró a nadie llevándose a cabo la diligencia, como en los demás, bajo la fe del Letrado de la Administración de Justicia.

La recurrente estuvo presente en el registro de su domicilio y no pudo estar en los demás porque los registros fueron simultáneos y porque, en principio, no era moradora de los demás domicilios y no estaba ni localizada ni tampoco detenida. Su detención se produjo precisamente en el momento de la práctica de la diligencia.

El artículo 569 de la LECrim dispone que el registro de un domicilio particular se hará a presencia del interesado o de la persona que legítimamente le represente. La jurisprudencia de esta Sala ha sido vacilante a la hora de precisar qué deba entenderse por " interesado" ya que en alguna sentencia se ha tenido por tal a la persona titular del domicilio afectado, en cuanto titular del derecho a la intimidad afectado por la injerencia

(SSTS. 18.7.98, 16.7.2004, y 3.4.2009), mientras que en otras sentencias se ha considerado que tiene ese carácter la persona que es objeto de la pesquisa policial, en tanto directamente interesa en el resultado del registro por las repercusiones procesales y penales que de su desarrollo se pueden derivar (SSTS 27.10.99, 30.1.2001 y 26.9.2006). Esta última postura es la mayoritaria de forma que se precisa la presencia del interesado en la diligencia por más que no sea el titular del domicilio en el supuesto de que ese interesado esté detenido. En la STS 771/2010, de 23 de septiembre, seguida por otras muchas, se declaró que ciertamente la jurisprudencia es uniforme en exigir la presencia del interesado-persona investigada- en la realización del registro en aquellos casos en los que se halle detenido y aun en el supuesto en que sea distinta del titular del domicilio o este se halle presente o rehúse su presencia en la diligencia. Tal presencia, si es posible, viene reclamada por las exigencias contradictorias de que debe de rodearse toda diligencia de prueba y más por las características de los registros domiciliarios en los que la ausencia de contradicción en el acto del mismo en que se lleva a cabo no puede cumplirse por la actividad contradictoria que posibilita el debate del juicio oral. Por tanto, de encontrarse detenido el interesado, su presencia en el registro es obligada, no siendo de aplicación las excepciones establecidas en los párrafos 2 y 3 del art. 569 LECrim (SSTS. 833/97 de 20.6, 40/99 de 19.1, 163/2000 de 11.2, 1944/2002 de 9.4.2003).

Ahora bien, hay supuestos en que esa presencia no es posible y son variadas las circunstancias que pueden imposibilitar esa presencia: Que el investigado no esté localizable, que no quiera asistir en caso de no estar detenido y que no pueda físicamente hacerlo, como ocurre en casos de registros simultáneos. En este último caso así se ha reconocido por esta Sala en numerosas sentencias de las que podemos citar las SSTS 947/2006, de 26 de septiembre, 771/2010, de 23 de septiembre y 199/2011, de 30 de marzo.

En este caso la recurrente estuvo presente en el registro de su vivienda y no lo estuvo en los demás registros porque se practicaron de forma simultánea.

El motivo en consecuencia, se desestima, resultando confirmada en todos sus extremos la sentencia recurrida.

Conclusiones.

En pocas ocasiones el TS ha mantenido una línea tan uniforme sobre quién debe tenerse por interesado en una entrada y registro, siendo aquél el que con independencia del título formal que ostente respecto al domicilio, pueda resultar afectado jurídicamente con su resultado en el delito que se investiga. También desgrana los problemas prácticos entre los registros sucesivos y los simultáneos para que el interesado puede acudir a esa diligencia, salvo que por motivos excepcionales o de fuerza mayor no sea viable.

2.- STS 358/2025, de 10 de abril de 2025. Noticia criminal traslada a España por una autoridad judicial extranjera y continuación de la investigación en nuestro país con nuevas pesquisas policiales[2].

Antecedentes de hecho

En el rollo nº 33/2021 (dimanante del PA 25/2021 del Juzgado de Instrucción nº 3 de Talavera), seguido ante la Audiencia Provincial de Toledo, Sección 1ª, con fecha 5 de mayo de 2022 se dictó sentencia condenatoria para Evelio como autor de un delito contra la salud pública por tráfico de drogas, que contiene los siguientes hechos probados:"…Como consecuencia de una comunicación remitida por la Fiscalía de Portugal se tuvo conocimiento que podía existir un grupo organizado que desde Sudamérica se encarga de enviar cocaína a Europa, al menos a España y Portugal, y que para ello utilizaba barcos que recalaban en el puerto de Oporto. Y desde dicha localidad se producía, al menos en parte, el traslado, por medio de camiones, hasta la localidad de Talavera La Nueva, en donde era descargada en una nave industrial con el rótulo Puertas Artevi. A resultas de esa información por parte de la Udyco se inició una investigación que dio como resultado el comprobar que la información, en cuanto a la llegada de camiones a la nave, era cierta por lo que iniciaron una serie de vigilancias y seguimientos que les permitieron conocer que la nave estaba alquilada por el acusado Evelio, nacido en 1984, sin antecedentes penales, quien tenía también alquilada una nave en la localidad de Ventas de Retamosa y un trastero, con el número, propiedad de la empresa Blue Space, de Leganés. Por auto de 22 de diciembre de 2020 el Juzgado de Primera Instancia e Instrucción número Tres de los de Talavera se autorizó la entrada y registro en las referidas naves y en el trastero. En este fueron hallados siete paquetes rectangulares, conteniendo una sustancia blanca, a la que se le aplicó el reactivo adecuado dando positivo a la cocaína. Tras el correspondiente análisis la sustancia resultó ser cocaína, con un peso total de seis mil noventa y seis gramos y una riqueza media del 77,88%, y cuyo valor en el mercado ilícito ascendería a la suma de doscientos treinta y ocho mil trescientos sesenta y nueve con treinta y un euros, que el acusado poseía para su distribución entre tercero. No ha quedado probado que los otros acusados, Gaspar, nacido el NUM002 de 1969, sin antecedentes penales, y Jacinta, nacida en 1991, ejecutoriamente condenada en sentencia de 16 de junio de 2020 por delito contra la salud pública, tuvieran relación con la sustancia intervenida…"

Fundamentos jurídicos

Solicita el recurrente en casación, la nulidad del auto que acordaba la intervención de los teléfonos del acusado, y del auto de 29 de julio de 2020, por el que se acordó su prórroga así como nuevas intervenciones, peticiones que por primera vez se hicieron como cuestión previa al inicio del juicio oral, y ya fueron rechazadas por el tribunal de instancia con acertados argumentos.

El motivo como decimos, coincide con el esgrimido en apelación con la sola diferencia de que transcribe un párrafo de la STSJ, pero con la que no debate, repite que

[2] STS 35872025, de 10 de abril de 2025, publicada en la web del CGPJ por el Centro de Documentación Judicial, CENDOJ, (ROJ: STS 1628/2025 - ECLI:ES:TS:2025:1628). recurso: 8375/2022. Ponente Excmo. Sr. D. Ángel Luis Hurtado Adrián.

esa nulidad de los referidos autos se sustenta en la ausencia de motivación y justificación, al carecer de objeto y desbordar las previsiones contenidas en el marco de colaboración por parte de las autoridades españolas con las portuguesas, y la irregularidad que se atribuye a dichos autos es porque las personas donde se iría a almacenar y esconder la droga ya estaban identificadas por medio de vigilancias policiales llevadas a cabo los días 14, 15, 17 y 19 de mayo, por lo que, en opinión del recurrente, carece de fundamento y no tiene base jurídica solicitar por la fuerza actuante, y que se autoricen intervenciones telefónicas 25 días después.

Se alega que el objeto de las vigilancias estaba en torno a la llegada desde Portugal de un camión con un cargamento para depositarlo en la nave el 14 de mayo de 2020, y que, teniendo vigilada la llegada y descarga, lo lógico es que la intervención policial se hubiese llevado a cabo ese día o los posteriores y que si no se lleva a cabo, es porque no se tiene certeza de que ahí viniese la droga, de manera que si es así y 25 días después se acuerdan las intervenciones telefónicas, considera quien firma el recurso que se trata de una investigación prospectiva, porque en ese momento no se tiene constancia de que se esté cometiendo o se vaya a cometer algún delito, y vuelve repetir que, cuando se dicta el auto cuestionado, no existía ninguna «buena razón» o «fuerte presunción» que justificase esa intervención, y lo hace sin oponer argumento alguno a las consideraciones que, para rechazar tal planteamiento, le dio primero, la sentencia de instancia y, después la de apelación, cuando está reiterando, una vez más, una pretensión de consecuencias tan traumáticas como es una nulidad por considerar prospectiva la investigación, a la que bastante más extensión debería haber dado tras habérsela rechazado en dos ocasiones anteriores.

El planteamiento por el que discurre el recurrente parte de vincular la actuación policial que tiene lugar a partir del día 14, a raíz de información recibida de las autoridades portuguesas, con la investigación a que se contrae la presente causa, y así resulta de la misma lectura de los hechos probados, en que se habla de la comunicación remitida por la Fiscalía de Portugal, que permitió conocer la existencia de un grupo organizado que se encargaba de enviar cocaína a Europa, que llegaba por el puerto de Oporto y desde allí se trasladaba, al menos en parte, a la nave industrial con el rótulo Puertas Artevi de la localidad de Talavera de la Reina, alquilada por Evelio, en torno al cual se estaba llevando una investigación en Portugal, que dio lugar a la emisión por parte de la Fiscalía de Oporto de una Orden Europea de Investigación, en solicitud de determinadas diligencias en nuestro país, y que, como se recoge en auto de 22 de diciembre de 2020, mediante auto de 29 de junio de 2020 se acordó reconocer y ejecutar, entre cuyas diligencias se encontraba la intervención de determinados teléfonos, entre ellos el del referido Evelio, intervención que fue prorrogada mediante auto de 29 de julio de 2020 y fue dejada sin efecto por auto de 18 de septiembre de 2020, investigación portuguesa en que no consta que hubiera llegado a estar encartado éste.

Las pesquisas policiales continuaron en nuestro país, a través de la Udyco, mediante la práctica de vigilancias y seguimientos, constatando que, entre otros, el referido Evelio llevaba a cabo medidas de seguridad que en el auto se recogen, indicativas de una presumible actividad delictiva relacionada con un delito de tráfico de drogas, distinta y posterior a la que pudiera ser objeto de investigación en Portugal, pues, como explica la sentencia de instancia , «no consta que contra los acusados se instruyese causa en el país vecino por lo que la instrucción no podía circunscribirse solo a la identificación de los

posibles autores que en España han cometido los hechos que son objeto de procedimiento penal en Portugal».

En cualquier caso, la información inicial aunque viniera de Portugal, aportaba elementos que justificaban la adopción de medidas que tomó la juez de instrucción, incluida la limitativa de derechos fundamentales, como fue la intervención telefónica acordada, que por lo tanto, no se puede considerar que fuera dada en el curso de una investigación prospectiva, pero a la vez era de utilidad en orden a la investigación por la presumible actividad delictiva que se estuviera cometiendo en España, y el que se mantenga lo contrario, como argumenta el M.F., es «razonamiento difícil de mantener, por cuanto que parece afirmar el recurrente, que en la investigación de un delito del que se tiene noticia previa, se tiene que renunciar a investigar la existencia de otros posibles partícipes, en un delito tan grave como en el presente caso».

Con precisión lo explica la sentencia recurrida, que expone las razonas por las cuales se ha de desvincular los hechos que se investigan en Portugal con los que debían investigarse en nuestro país, aunque en ambos estuvieran relacionados con delitos de tráfico de drogas, porque la ruptura que hay entre ambos es evidente, y cada cual, haciendo nuestras las palabras que acabamos de transcribir tomadas del M.F., debía lugar a su propia investigación, y así lo explica, también, la sentencia recurrida, que diferencia entre la investigación portuguesa y la española, cuando dice que «la instrucción no tenía por qué circunscribirse solo a la identificación de las personas y lugar en el que escondían droga, porque no se trataba de una colaboración con las autoridades portuguesas respecto de unos hechos que fueran objeto de un procedimiento penal en Portugal, ni consta causa penal contra los acusados en dicho país, sino que se trataba de una información dirigida por la Fiscalía portuguesa a la policía española sobre unos hechos de los que se deducía la posible comisión de un delito en España, incorporando datos objetivos indiciarios de actividad delictiva en nuestro país, como es la llegada de un barco, la carga de bobinas, las empresas transportistas y, sobre todo, el destino en España del material cargado en Portugal».

En resumen, contando como contaba la Jueza de Instrucción con elementos indiciarios con la suficiente verosimilitud como para apreciar la presumible comisión de un delito de tráfico de drogas en nuestro país, aunque fueran aportados por una información venida de Portugal, no cabe hablar de investigación prospectiva, porque esa información es la que le aportaba esos elementos, en consonancia con los cuales adoptó las medidas de investigación que consideró oportunas, entre ellas la intervención del teléfono de uno de los presumiblemente implicados en ella, que motivó con la suficiente extensión en su auto de 29 de junio de 2020 y también en el de prórroga de 29 de julio de 2020.

El recurso de casación resulta desestimado en su integridad y mantiene la condena del recurrente.

Conclusiones.

Valora el TS el alcance de una OEI remitida formalmente desde la autoridad judicial portuguesa a la autoridad judicial nacional, como instrumento de cooperación que llevaba aparejada algunas medidas restrictivas de derechos fundamentales. Cuando esa línea de investigación no prosperó y finalizó, y tampoco se siguió en Portugal un procedimiento

penal independiente sobre los mismos hechos, la Policía Judicial española añadió a esa información nuevos datos de los investigados y de posibles hechos delictivos cometidos en España, e inició un procedimiento que tomando como base el primero, permitió desarticular un grupo criminal dedicado a la comisión de delitos graves.

3.- STS 324/2025, Penal sección 1 del 07 de abril de 2025. Conservación de datos de las comunicaciones[3].

Antecedentes de hecho

La Audiencia Provincial de Barcelona, Sección 7ª dictó sentencia nº 173/2023 de 3 de marzo, dimanante del sumario nº 1/2021 del Juzgado de Instrucción nº 1 de Sant Boi de Llobregat, seguido por delito contra la salud pública, que contiene entre otros los siguientes hechos probados:"…son hechos probados, y así se declara, que desde al menos en el mes de agosto de 2018 los procesados Jenaro, Humberto, Fermín, Lucas y Emiliano formaron un entramado personal, material, societario y logístico puesto al servicio de un plan común que era hacerse con la cocaína oculta en un contenedor procedente de Brasil que llegaría al puerto de Barcelona a mediados de diciembre, para proceder a su distribución en esta última provincia. Jenaro estaba en la cúpula de dicho entramado aportando al mismo cobertura económica y contactos para conseguir la droga; Humberto ejercía funciones de dirección y coordinación. Fermín sumaba la estructura societaria y empresarial capaz de hacerse con tal cargamento haciéndolo pasar por una compraventa lícita de folios Din-A4, Lucas la logística, concretada sobre todo en la organización del transporte de la sustancia del que se encargaría Emiliano, delegándolo en terceros.

En ejecución de dicho plan criminal la empresa Campderros Salvans S.L., adquirió por mediación de Fermín, 1.600 cajas de folios DIN-A4 a la empresa Precisión Comercio Internacional LTDA con sede en Pinheiro- Maceió (Brasil), estando prevista su llegada al Puerto de Barcelona en el mes de diciembre de 2018; mercancía que fue repartida en dos contenedores con 800 cajas de folios DIN-A4 cada uno, contenedores con numeración APZU3035695 y APZU3807079 fletados a bordo del barco de la naviera CMA-CGM RÍO GRANDE, zarpando del Puerto de ltaguaí (Río de Janeiro-Brasil) con destino al Puerto de Barcelona, en fecha 21 de noviembre de 2018…" Continúa el relato de hechos probado diciendo que, "…A las 13:40 horas de la referida fecha, durante las labores de carga y redistribución de los paquetes de folios en el camión que manejaba Herminio, cayó accidentalmente de la carretilla mecánica empleada por uno de los trabajadores de Campderros Salvans S.L., Nemesio, una caja de folios que salía del contenedor con numeración APZU 3035695, la cual, al romperse, dejó al descubierto varios paquetes rectangulares que resultaron contener la sustancia estupefaciente mentada. Requerida la presencia policial, se personó en el lugar una dotación de agentes de los Mossos d'Esquadra, que, tras inspeccionar debidamente la totalidad de las cajas de folios, localizaron en su interior los 1.410 paquetes rectangulares que presentaban las siguientes características identificativas…"

[3] STS 324/2025, Penal sección 1ª del 07 de abril de 2025, publicada en la web del CGPJ por el Centro de Documentación Judicial, CENDOJ, (ROJ: STS 1487/2025 - ECLI:ES:TS:2025:1487). Recurso: 10408/2024. Ponente Excmo. Sr. D. Manuel Marchena Gómez.

Fundamentos jurídicos

En una larga sentencia, el TS desgrana las numerosas impugnaciones de las defensas de los condenados que intentan desmontar el acierto del razonamiento condenatorio, destacando incluso que uno de los recurrentes censura al Juez instructor que no hubiera añadido a la injerencia que de por sí representa la intervención telefónica otras medidas que reforzaran la intromisión del Estado en el círculo de exclusión definido por el derecho a la intimidad. No tiene sentido reivindicar la nulidad de un acto jurisdiccional de intromisión en la vida privada de un sospechoso reprochando al Juez que no haya autorizado limitaciones todavía más intensas de las que se consideraron necesarias y proporcionadas.

En pocas ocasiones como en el presente caso, cualquier queja de una posible investigación prospectiva o contraria a los principios de proporcionalidad, necesidad o excepcionalidad -art. 588 bis a- ha de ser necesariamente descartada.

A partir del hallazgo casual de la droga por un accidente en las labores de descarga, el trabajo de las Fuerzas y Cuerpos de Seguridad del Estado dirigido a conocer quién había adquirido para su distribución clandestina ese extraordinario cargamento de cocaína estaba plenamente justificado. Ese trabajo, además, contó con el control limitativo del Juez de instrucción núm. 1 de Sant Boi de Llobregat y la intervención fiscalizadora del Fiscal (art. 306 de la LECrim).

Ahora nos centramos en la impugnación de la conservación de datos de las comunicaciones.

El motivo incorpora una alegación referida a la solicitud de los Mossos a las operadoras de telefonía de conservar los datos más allá del plazo de expiración de 1 año impuesto por la Ley 25/2007, 18 de octubre, de conservación de datos, con una referencia marginal a la sentencia del Tribunal de Justicia de la Unión Europea de 8 de abril de 2014, que declaró la nulidad de la directiva 2006/24/CE.

Alega la defensa que la petición de conservación de esos datos -que no fue formalmente incorporada a la causa- no fue autorizada con carácter previo por el Juez de instrucción.

La sentencia recurrida reprocha al recurrente que esa nulidad se pretenda mediante una alegación genérica en la que no se dice cuál es el auto o línea intervenida que quedaría afectada". Y razona que la autorización judicial está implícita en las resoluciones habilitantes que implican, por su propia naturaleza, la necesidad de que los datos vinculados a esos procesos de comunicación sean conservados.

En cualquier caso, la Sala estima que esa autorización judicial para requerir a las operadoras o a cualquier otra persona física o jurídica la conservación de los datos no es preceptiva.

Así se desprende de lo previsto en el art. 5 de la Ley 25/2007, 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones. Y así se infiere también del art. 588 *octies* de la LECrim, en el que

se regula la orden anticipada de conservación de los datos como medida de aseguramiento.

El primero de estos preceptos tiene como destinatarios a los operadores que presten servicios de comunicaciones electrónicas disponibles al público o exploten redes públicas de comunicaciones, en los términos establecidos en la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones", criterio reiterado en el art. 1 de la vigente Ley 9/2014, 9 de mayo, General de Telecomunicaciones.

El segundo - art. 588 octies de la LECrim - incorpora el mismo deber de aseguramiento y preservación de los datos cuando el depositario es una persona física o jurídica y en él se excluye de forma explícita la necesidad de autorización judicial: "el Ministerio Fiscal o la Policía Judicial podrán requerir a cualquier persona física o jurídica la conservación y protección de datos o informaciones concretas incluidas en un sistema informático de almacenamiento que se encuentren a su disposición hasta que se obtenga la autorización judicial correspondiente para su cesión con arreglo a lo dispuesto en los artículos precedentes".

Por consiguiente, tanto el Fiscal como las Fuerzas y Cuerpos de Seguridad del Estado están facultados para cursar, sin necesidad de autorización judicial, esa orden de conservación que, como es lógico, sólo adquiere sentido en el marco de una investigación en la que se haga previsible la ulterior necesidad de incorporación de esos datos al proceso penal iniciado.

La no exigencia de autorización judicial se desprende no sólo de la literalidad de ese precepto, sino de la exposición de motivos de la propia LO 13/2015, 5 de octubre, que introdujo el art. 588 octies, cuando decía que, finalmente y por lo que se refiere a las diligencias de investigación tecnológica, la reforma contempla como medida de aseguramiento la orden de conservación de datos, cuyo fin es garantizar la preservación de los datos e informaciones concretas de toda clase que se encuentren almacenados en un sistema informático hasta que se obtenga la autorización judicial correspondiente.

Conclusiones

Distingue claramente esta STS entre una medida de conservación de datos y otras tecnológicas propiamente dichas, deslindando cuando es preceptiva la autorización judicial y cuando pueden actuar directamente las FCSE. Medidas tecnológicas previstas en los art. 588 bis y siguientes de la LECrim que están en algunos casos con una importante falta de actualización normativa, como el uso de drones, el uso de la IA…

4.- STS 294/2025, de 28 de marzo de 2025. Alcance del principio de insignificancia y de toxicidad en los delitos contra la salud pública[4].

Antecedentes de hecho.

El Juzgado de Instrucción nº 11 de Palma de Mallorca, incoó diligencias previas nº 649/2020, una vez concluso lo remitió al Juzgado de lo Penal nº 2 de Palma de Mallorca, para su enjuiciamiento en el procedimiento abreviado nº 11/2022, quien dictó Sentencia nº 111/2022, de fecha 28 de marzo de 2022, que contiene los siguientes hechos probados: "…ÚNICO.- Probado y así se declara que el acusado Lázaro, mayor de edad, sin antecedentes penales y privado de libertad por esta causa el día 9 de julio de 2020, sobre las 00:15 horas del día 9 de julio de 2020 se encontraba en la Calle General García Ruiz de Magalluf, contactando con un turista británico al que le ofreció cocaína a cambio de 50€, entregándole un envoltorio con dicha sustancia, recibiendo la cantidad de 50€, hecho que fue observado por una dotación de la policía local de Calviá que pararon su vehículo y se dirigieron hacia donde había ido el súbdito británico junto con un amigo, encontrándolos sentados esnifando la sustancia y les dijeron que acababan de comprar cocaína a un joven de color y que habían pagado 50€, intentando ocultar con los pies la cocaína que quedaba en el envoltorio, seguidamente fueron en dirección contraria y procedieron a interceptar a Lázaro interviniéndole en la cartera 50€ y en la tela del pantalón donde llevaba un cordón a modo de cinturón la cantidad de 50€ más. La sustancia que quedaba en el envoltorio una vez analizada resultó ser cocaína de una pureza del 19,15% siendo su valor de venta de 4,83€…"

La sentencia del Juzgado de lo Penal fue recurrida en grado de apelación ante la Audiencia Provincial que desestimó el recurso. El TS estima la casación y dicta una sentencia absolutoria.

Fundamentos jurídicos.

La jurisprudencia admite la atipicidad de las conductas de tráfico cuando, debido a su absoluta nimiedad, la sustancia ya no constituya por sus efectos, una droga tóxica o sustancia estupefaciente, sino un producto inocuo por su precaria toxicidad (SSTS 527/1998, de 15 de abril; 985/1998, de 20 de julio; 789/99, de 14 de abril; 1453/2001, de 16 de julio; 1081/2003, de 21 de julio; y 14/2005, de 12 de febrero). El principio de insignificancia reclamaría la impunidad cuando la cantidad de droga es tan exigua que resulta incapaz de producir efecto nocivo alguno en la salud. Falta antijuridicidad material por ausencia de un verdadero riesgo para el bien jurídico protegido (SSTS 1441/2000, de 22 de septiembre; 1889/2000, de 11 de diciembre; 1591/2001, de 10 de diciembre; 1439/2001, de 18 de julio; y 216/2002, de 11 de mayo).

Por otra parte, conviene precisar que nuestra más reciente jurisprudencia ha matizado el uso del término "insignificancia"; se prefiere hablar de "toxicidad". Lo que cae fuera del tipo penal son las transmisiones de sustancias que por su falta de lesividad no entrañarían riesgo.

[4] STS 294/2025, Penal sección 1ª del 28 de marzo de 2025, publicada en la página web del CGPJ, Centro de Documentación Judicial, CENDOJ, (ROJ: STS 1335/2025 - ECLI:ES:TS:2025:1335), recurso: 6755/2022. Ponente Excma. Sra. Dña. Susana Polo García.

Esta doctrina ha de aplicarse de forma excepcional y restrictiva, pero con certeza. En este contexto, esta Sala sigue operando con los criterios establecidos en el Pleno de 24 de enero de 2003. Así lo constatan múltiples precedentes (SSTS 936/2007, de 21 de noviembre; 1110/2007, de 19 de diciembre; 183/2008, de 29 de abril; y 1168/2009, de 16 de noviembre) (vid. la STS 587/2017, de 20 de julio).

Ahora bien, con respecto al concepto de mínimo psico-activo, y sus repercusiones penológicas en el elemento subjetivo del delito, la STS 1982/2002, de 28 de enero de 2004, nos dice que los mínimos psico-activos son aquellos parámetros ofrecidos por un organismo oficial y de reconocida solvencia científica, como es el Instituto Nacional de Toxicología, que suponen un grado de afectación en el sistema nervioso central, determinando una serie de efectos en la salud de las personas, desde luego perjudiciales, al contener unos mínimos de toxicidad, y producen también un componente de adicción, que ocasiona que su falta de consumo incite hacia la compulsión. Se trata, pues, de drogas que ocasionan daño en la salud pública, entendida ésta como la de los componentes de la colectividad en su aspecto individualizado, y cuya pena se diseña por el legislador penal, según que tal afectación (daño) sea grave o no. Esos mínimos suponen que la cantidad transmitida es algún tipo de sustancia estupefaciente, tóxica o psicotrópica incluida en los convenios internacionales en la materia, mediante los listados al efecto. Colman, pues, el tipo objetivo del delito, e inciden tanto en la antijuridicidad formal, como en la material. Tales mínimos han sido ofrecidos por informe del Instituto Nacional de Toxicología, y dentro de los márgenes que permite tal peritaje, pueden ser interpretados, sin que se requiera necesariamente automatismo judicial alguno (STS 580/2017, de 20 de julio).

Es decir, cualquier sustancia estupefaciente que supere la dosis mínima psicoactiva, genera el prejuicio para la salud que la norma típica sanciona y que consecuentemente si es gravemente perjudicial para la salud por su naturaleza y catalogación, sigue siéndolo, cualquiera que sea la cantidad y pureza (o grado de adulteración, si se prefiere), una vez superado ese mínimo psicoactivo (STS 723/2017, de 7 de noviembre).

En todo caso, porque sobre esta materia hay que recordar nuestra doctrina jurisprudencial, que tuvo su origen en el Pleno no Jurisdiccional de 24 de enero de 2003 que, en relación a la cocaína, estableció que su principio activo opera a partir de los 50 miligramos (0,05 gramos); criterio que fue el aceptado por la Sala y recogido en el Pleno no Jurisdiccional de 3 de febrero de 2005 en el que se tomó el acuerdo de "continuar manteniendo el criterio del Instituto Nacional de Toxicología relativo a las dosis mínimas psicoactivas, hasta tanto se produzca una reforma legal o se adopte otro criterio o alternativa".

En efecto, como indica el recurrente, en el relato fáctico no consta la cantidad de cocaína intervenida, además, según el informe del Área de Sanidad de la Delegación de Gobierno de las Illes Balears la sustancia intervenida policialmente fue 0,093 gramos de cocaína. Por tanto, si como consta en los hechos probados la pureza es de 19,15%, nos encontramos con un total de 0'017 gramos de cocaína neta, esto es, 17 miligramos, cantidad claramente inferior a los 50 miligramos a partir de los que existe el riesgo para la salud pública.

Si bien es cierto que en el relato fáctico se relaciona de una forma incompleta un acontecimiento que podría constituir, en su conjunto, un acto de tráfico, lo cierto es que finalmente solo se declara probada la ocupación al supuesto comprador - no identificado,

pese a que los policías manifiestan haber hablado con él- de una cantidad infinitesimal de droga, 0,093 gramos, con una pureza de 19,15%, por tanto, nos encontramos con un total de 0'017 gramos de cocaína neta -17 miligramos-, cantidad inferior a la dosis mínima psicoactiva, sin considerar expresamente acreditada la ocupación de otras sustancias estupefacientes al acusado, por lo que no puede inferirse, razonablemente, de dicha mínima cantidad, la dedicación al tráfico y, sobre todo, debe estimarse que carece de relevancia penal por su inocuidad para la salud pública.

Conclusiones.

A pesar de la claridad del relato de los hechos probados, un acto de tráfico de drogas al menudeo en el que se detalla la función del comprador y del vendedor, nada nuevo aporta esta STS a la línea jurisprudencial ya seguida hace lustros y que se mantiene invariable, sobre el principio de insignificancia que ahora amplía con el calificativo de toxicidad, cuando se trata de aplicar el criterio del INTCF sobre las dosis mínimas psicoactivas para apreciar la tipicidad penal.

5.- SAN 8/2025, de 2 de abril de 2025. Delito de estragos con fines terroristas[5].

Antecedentes de hecho.

Las presentes actuaciones judiciales se iniciaron en virtud de comunicación vía fax de la Secretaría de Estado de Interior, TEPOL, informando de la explosión de un artefacto de forma controlada en el Aeropuerto de "El Altet" de Alicante, dictándose por el Juzgado Central de Instrucción número 2 de Madrid auto de incoación de diligencias Previas de fecha 31 de julio de 1995, y tras la instrucción correspondiente, se dictó auto de procesamiento de fecha 19 de mayo de 2010 contra Melisa por los delitos de estragos terroristas en grado de frustración.

Fundamentos jurídicos.

Relata esta sentencia de la Audiencia Nacional, que en el acervo probatorio en las actuaciones nos encontramos en primer lugar con un informe de la Comandancia de la Guardia Civil de Guipúzcoa de 10 de mayo de 2001, folio 294 y ss del tomo I de las actuaciones, en las que se informa al Juzgado Central de Instrucción que la procesada, en otras diligencias (26/01) también de dicha Comandancia, reconoce expresamente que había colocado el artefacto en el Aeropuerto de Alicante junto con otra persona (a quien no se juzga) dentro de una bolsa y en el interior de una papelera. Estas manifestaciones obran en su segunda declaración realizada en dependencias de la Guardia Civil el 31 de marzo de 2001 (folio 163 del tomo I de las actuaciones), diciendo además que fue el mismo día que colocó otro artefacto en la oficina de Turismo de Denia…

Llegados al juicio y tras una encomiable labor de la Guardia Civil, existe un vacío probatorio incomprensible que denuncian los propios miembros del Tribunal y dice así, "…No obstante lo anterior, y a pesar del esfuerzo realizado por el Ministerio Fiscal, entendemos que existe un vació probatorio importante que hace que debamos declarar la absolución de la procesada. Un vacio probatorio que proviene de la falta y ausencia de

[5] SAN 8/2025, Penal sección 3ª del 02 de abril de 2025, publicada en la página web del CGPJ, Centro de Documentación Judicial, CENDOJ, (ROJ: SAN 1662/2025 - ECLI:ES:AN:2025:1662). Recurso: 132/2010. Ponente Excmo. Sr. D. Jesús Eduardo Gutiérrez Gómez.

prueba de un dato previo trascendental, como lo es la autoría de la carta manuscrita que el Ministerio Fiscal atribuye a Melisa, y respecto de lo cual no se ha practicado prueba alguna. Este vacío probatorio viene dado por la falta de proposición de la prueba correspondiente de los funcionarios de Policía que emitieron el informe pericial caligráfico que obra en las actuaciones en el denominado "Anexo de Documentación", y donde se analiza pormenorizadamente los documentos encontrados en Francia, entre los cuales figura la "kantada" que se atribuye a la procesada. Tal informe pericial caligráfico de fecha 20 de mayo de 2008 y elaborado por los funcionarios de Policía con carnet profesional número NUM005 y NUM006, fue ratificado en la fase de instrucción ante el Juzgado Central de Instrucción, pero posteriormente el Ministerio Fiscal no los propuso como prueba pericial, por lo que al no haber sido "traídos" a juicio, y no haber sido sometido a contradicción entre las partes, no se puede tener como prueba de cargo contra la procesada, habiendo sido expresamente impugnado por su defensa, procesada que, por otra parte, en el plenario manifestó de manera clara y patente que no reconocía como suyo el documento en cuestión y que no lo había escrito. Por otro lado, el informe 7/2015, informe que podríamos denominar "informe de inteligencia" donde se analiza la existencia y componentes del comando de ETA denominado Ibarla, la actividad del mismo, y los datos de los atentados cometidos por este comando terrorista, y su comparativa con los documentos encontrados en Francia, así como con declaraciones policiales, tampoco ha sido objeto de prueba en el plenario, ya que tampoco fueron propuestos como peritos los autores del mismo, informe que podría haber arrojado luz acerca de la posible autoría de la colocación del explosivo en el Aeropuerto de Alicante, frente a la negación de la procesada de los hechos. No tienen, pues, valor probatorio como prueba de cargo y como prueba que acredite la autoría de la procesada las declaraciones de los testigos que han comparecido al plenario, ya que, de manera errónea, se ha "presumido" y se ha dado por supuesto que la "kantada", única prueba sólida de cargo (la declaración policial no tiene valor como prueba de cargo ya que no ha sido contrastada ni ratificada por la procesada en el juzgado Central de Instrucción) la había escrito la procesada, por lo que el que se acrediten las posibles divergencias entre dicho documento y la declaración policial, no nos sirve de gran cosa, pues falta el requisito o la condición previa, el haberse acreditado la autoría de dicho documento.

En consecuencia, y sin entrar a valorar las demás pruebas, procede declarar la absolución de la procesada con toda clase de pronunciamientos favorables…"

Conclusiones.

Sangrante testimonio que recoge esta SAN nº8/2025 Sección 3ª, cuando la labor policial es impecable y el trabajo en la fase de instrucción más que completo. Craso error por el Ministerio Fiscal al no proponer en el plenario la declaración de los agentes que analizaron la documentación de la procesada y de los autores de la pericial de inteligencia. No había otra opción más que la libre absolución.

6.- STS 308/2025, de 2 de abril de 2025. Investigación policial en España que surge a partir del conocimiento de una OEDE dictada por las autoridades judiciales de otro país por otro hecho delictivo. Presencia de los detenidos en un registro domiciliario[6].

Antecedentes de hecho.

El Juzgado de Instrucción n.º 1 de Coín incoó procedimiento abreviado 22/2022 por delito contra la salud pública y tenencia ilícita de armas contra, entre otros, Clemente, David y Eliseo, que una vez concluido remitió para su enjuiciamiento a la Audiencia Provincial de Málaga, Sección 3ª. Incoado procedimiento abreviado 54/2022, con fecha 23 de noviembre de 2022 dictó Sentencia nº 362/22, en la que se contienen entre otros, los siguientes hechos probados:"…Probado y así se declara que las autoridades policiales de Málaga tuvieron conocimiento de que Clemente, mayor de edad, sin antecedentes penales computables, de nacionalidad británica sobre el que pesaba una orden internacional de detención emitida por las autoridades de Reino Unido, pudiera estar residiendo en esta provincia, concretamente en algún lugar del Valle de Guadalhorce o de Coín. Tras las investigaciones oportunas, los agentes encargados de la investigación llegaron a la conclusión de que pudiera estar residiendo en la dirección xxx de la localidad de Coín. Por dicho motivo se establecieron vigilancias policiales los días 3, 4 y 5 de Mayo de 2022, sobre el citado inmueble de la dirección xxx de Coín, donde los funcionarios policiales finalmente supieron con seguridad que vivía Clemente junto con otros hombres. Concretamente los días indicados, se encontraban en el interior del inmueble el citado Clemente, mayor de edad y sin antecedentes penales, junto David y Eliseo, todos ellos mayores de edad y sin antecedentes penales y Fidel, mayor de edad y sin antecedentes penales computables, quien se incorporó a la citada vivienda en algún momento situado entre la noche del día 3 de mayo, que salió de prisión, y las 20.35 horas del día 5 de mayo en que fue visto abandonar la vivienda para dirigirse a un centro deportivo. De todos ellos, eran David y Eliseo quienes salían del inmueble para realizar las compras necesarias, y lo hacían usando un vehículo Volkswagen polo de matrícula inglesa, adoptando en la conducción medidas de seguridad para comprobar si eran seguidos tales como dar varias vueltas a las rotondas o no estacionar el vehículo en la puerta del inmueble sino en las inmediaciones de la vivienda.

El día 5 de mayo sobre las 20:35 horas, Clemente, Fidel, David y Eliseo salieron juntos de la vivienda, cerrando la puerta de la vivienda con llave Fidel, quien en ese momento llevaba en la espalda una mochila negra que durante el trayecto se la entregó a Clemente. Las cuatro personas citadas se dirigieron al Gimnasio BlueLife Sportclub y Spa, situado en el Centro Comercial La Trocha ubicado en Coín, siendo en este momento cuando los agentes de policía intervinieron para detener a los cuatro hombres citados. En el momento de la detención, la mochila negra que a la salida de la casa portaba en su espalda Fidel estaba situada a los pies del éste y de Clemente. En el interior de la mochila tras su inspección se encontró una pistola calibre 9mm Parabellum de marca Ruger modelo P89 municionada y sin seguro con número de serie eliminado. Tras el pertinente análisis la misma estaba en correcto estado de conservación siendo su funcionamiento mecánico y operativo también correcto tanto en simple como en doble acción, siendo apta

[6] STS 308/2025, Penal sección 1ª del 02 de abril de 2025, publicada en la página web del CGPJ, Centro de Documentación Judicial, CENDOJ, (ROJ: STS 1482/2025 - ECLI:ES:TS:2025:1482), recurso: 11312/2023. Ponente Excmo. Sr. D. Pablo Llarena Conde.

para el disparo. Ni Fidel, ni Clemente, ni David ni Eliseo estaban en posesión de licencia de dicha arma.

El día 6 de mayo 2022 se dictó auto por el juzgado de Coín autorizando la diligencia de entrada y registro de la vivienda de la dirección xxx de Coín por auto 6 de mayo de 2022 en el que se encontró una importante cantidad de estupefaciente…"

Fundamentos jurídicos

Resulta sorprendente que las Defensas de los condenados no plantearan la posible nulidad de las actuaciones desarrolladas por la Policía Judicial, cuando a sabiendas de la existencia de una OEDE, orden europea de detención y entrega, inician una investigación y no procedieran a la inmediata detención del requisitoriado. Nada dice la sentencia y mejor, porque avala todo el trabajo policial del que se da cuenta inmediata al Juez Instructor que acuerda incluso la diligencia de entrada y registro domiciliaria por el hecho seguido en España. Como veremos la sentencia de la AP de Málaga es condenatoria y la STS desestima el recurso de casación.

Esta es la información matriz de la causa que se traslada al Juzgado de Coín y que tantas veces vemos que puede suceder en la práctica, como por ejemplo, la existencia no ya de OEDE sino de buscas y capturas a nivel nacional y que nos haría pensar en la necesidad inmediata de detener cuando no siempre es así y vemos en esta STS.

Alegaban los recurrentes que es nula de pleno derecho la diligencia de entrada y registro practicada el día 6 de mayo de 2022 en la casa sita en la dirección xxx de la localidad de Coín, porque siendo la residencia habitual de los cuatro acusados y estando todos ellos detenidos, los agentes policiales únicamente condujeron a Fidel para que estuviera presente en su práctica. Consideran por ello que son nulos los resultados de tal diligencia de investigación y que no pueden utilizarse como prueba de cargo legítima, debiendo ser absueltos porque no existe ningún otro elemento probatorio que determine la responsabilidad de los recurrentes.

En las sentencias dictadas por esta Sala 420/2014, de 2 de junio, o 508/2015, de 27 de julio (caso Malaya), con cita de otros precedentes, sintetizamos nuestra doctrina sobre la exigencia de la presencia del interesado en la práctica de la entrada y registro domiciliario.

Decíamos en ellas que el fundamento de la exigencia de la presencia del interesado o de su representante en la entrada y registro domiciliario ordenada por la autoridad judicial en un proceso penal radica, en primer lugar, en que esta diligencia afecta a un derecho personal, de naturaleza constitucional, que es el derecho a la intimidad personal, ya que el domicilio constitucionalmente protegido, en cuanto morada o habitación de la persona, entraña una estrecha vinculación con su ámbito de intimidad, pues lo que se protege no es sólo un espacio físico sino, también, lo que en él hay de emanación de una persona física y de su esfera privada (STC 188/2013, de 4 de noviembre, en relación con el art. 18 2.º CE y el art. 8 CEDH). Y, en segundo lugar, en que afecta al derecho a un proceso con todas las garantías, porque el resultado de dicha diligencia constituirá prueba de cargo en el juicio contra el imputado cuyo domicilio se ha acordado registrar, lo que determina que en la práctica del registro se garantice la contradicción para asegurar la validez del registro como prueba preconstituida.

La Ley procesal prevé por ello, como requisito de la práctica del registro, la presencia del interesado o persona que legalmente le represente (art. 569 LECrim). Y el interesado a que se refiere el artículo 569 de la LECrim no es necesariamente el titular, en el sentido de propietario o arrendatario de la vivienda. Lo determinante no es quién sea el propietario, que puede ser desconocido, no residir en el domicilio, o incluso ser una persona jurídica, sino quién es el residente en el domicilio, pues es su intimidad la que va a ser afectada.

Ordinariamente el interesado en el registro es el imputado, pues el resultado del registro va a afectar a su defensa, aunque no siempre tiene que ser necesariamente el imputado la persona presente en el registro judicialmente autorizado. El imputado o persona contra la que se dirige el procedimiento puede encontrarse en ignorado paradero o simplemente fuera de la vivienda y no ser localizable en el momento del registro. La entrada y registro en un domicilio autorizada en el curso de un procedimiento judicial por delito constituye, por su propia naturaleza, una diligencia de carácter urgente que no se puede demorar a la espera de que el imputado regrese a su domicilio o sea localizado policialmente. Por ello la ley autoriza a prescindir del interesado "cuando no fuere habido", lo que resulta claramente referido al imputado, pudiendo en estos casos realizarse el registro ante cualquiera de sus familiares mayores de edad, estimando la doctrina jurisprudencial, atendiendo a una realidad social en la que las agrupaciones domiciliarias ya no se realizan necesariamente por familias en sentido estricto, que esta norma es aplicable a todos los moradores de la vivienda, mayores de edad, aunque no sean familiares en sentido estricto.

Ahora bien, decíamos, lo que sí que resulta exigible es la presencia del imputado en el registro cuando se encuentre detenido o a disposición policial o judicial, pues en estos casos no existe justificación alguna para perjudicar su derecho a la contradicción, que se garantiza mejor con la presencia efectiva del imputado en el registro.

En todo caso, también recordábamos en estas sentencias que esta regla no es aplicable a supuestos de fuerza mayor, en los que la ausencia de inculpado, pese a encontrarse a disposición policial, esté justificada. Citábamos como ejemplo los casos de hospitalización del imputado, o de detención en lugar muy alejado del domicilio, o bien en caso de registros practicados simultáneamente en varios domicilios. Y también cuando la imposibilidad de su presencia es de naturaleza jurídica, como por ejemplo cuando la instrucción haya sido declarada secreta (STS 143/2013, de 28 de febrero).

Y cuando son varios los moradores en la residencia, en nuestras SSTS 336/2017, de 11 de mayo o 913/2023, de 13 de diciembre, recordando las SSTS 698/2002, de 17 de abril, 1108/2005, de 22 de septiembre, 352/2006, de 15 de marzo, 684/2014, de 2 de octubre o 79/2015, de 13 de febrero, resaltamos que no se resiente la validez y eficacia de la diligencia de entrada y registro cuando se encuentre presente alguno de los moradores, siempre que el asistente no presente intereses contrapuestos a los del resto de encausados. Sin perjuicio de que, en esos supuestos, pese a la validez de la diligencia y para garantizarse el respeto al derecho a la contradicción que integra en el más amplio derecho de defensa, el registro no podrá ser valorado como prueba preconstituida y será preciso que, más allá de la mera lectura del acta levantada durante su realización, comparezcan a prestar declaración en el juicio oral los testigos que abordaron o presenciaron su práctica.

Lo expuesto determina la desestimación de los motivos.

Sin perjuicio de que en el presente supuesto la conducción y custodia de todos los privados de libertad hubiera resentido la disponibilidad de los efectivos policiales asignados a la pequeña población en la que los recurrentes desplegaban su actuación delictiva y en la que estaban detenidos, pues se hubiera precisado un elevado número de agentes para el traslado y la vigilancia de los cuatro encausados y para la realización de la diligencia de investigación, un análisis objetivo de las circunstancias concurrentes ofreció a los actuantes el fundamento de que no existía una contradicción de intereses entre los investigados. En concreto, el dispositivo de vigilancia policial, establecido durante tres días para el seguimiento prolongado de los habitantes de la vivienda, permitió constatar que todos ellos eran residentes en la casa y que todos ellos actuaban de manera concertada. En concreto, David y Eliseo, cuando salían de casa en coche, adoptaban medidas de seguridad para comprobar si eran seguidos. Y tanto estos como los otros detenidos actuaban en ocasiones de consuno y llegaron a intercambiarse algún objeto como una mochila. Y esta presunta ausencia de intereses contrapuestos se ha visto confirmada con las importantes cantidades de sustancias estupefacientes que se les incautó y con el número y la ubicación de las armas que fueron intervenidas, pues la prueba testifical, sometida a contradicción en el acto del plenario, refleja que la droga estaba a la vista de todos los habitantes de la casa y no estaba escondida en ninguna habitación destinada al uso exclusivo de alguno de ellos, desbaratándose así la posibilidad de que un responsable trate de trasladar su exclusiva responsabilidad a los demás residentes. Y así se incautaron también las tres pistolas que determinaron su condena como autores de un delito de tenencia ilícita de armas.

Conclusiones.

Después de avalar la instrucción en una causa que partía del conocimiento policial de una OEDE librada por las autoridades judiciales de Reino Unido por otro hecho delictivo distinto, y sin que las Defensas hubieran impugnado la posible omisión del deber de perseguir delitos por las FCSE al no detener inmediatamente a la persona sobre la que pesaba la OEDE vigente, y así evitar la investigación iniciada en el Juzgado de Coín, esta STS 308/2025 realiza una fenomenal y didáctica descripción de quién goza del concepto de interesado en una diligencia de entrada y registro domiciliario, estando o no detenido, fijando una regla general y las excepciones en casos extraordinarios. También delimita el posible conflicto de intereses entre los afectados.

7- STS 295/2025, Penal sección 1ª del 28 de marzo de 2025, delito de acoso, "stalking".[7]

Antecedentes de hecho.

El Juzgado de Violencia sobre la Mujer nº 1 de Medio Cudeyo, incoó diligencias urgentes nº 36/2021, una vez concluso lo remitió al Juzgado de lo Penal nº 5 de Santander, para su enjuiciamiento en el procedimiento juicio rápido nº 125/2021, quien dictó Sentencia nº 285/2021, de fecha 25 de noviembre de 2021, que contiene los siguientes hechos

[7] STS 295/2025, Penal sección 1ª del 28 de marzo de 2025, delito de acoso, "stalking", publicada en la página web del CGPJ, Centro de Documentación Judicial, CENDOJ, (ROJ: STS 1348/2025 - ECLI:ES:TS:2025:1348), recurso: 7251/2022. Ponente Excma. Sra. Dña. Susana Polo García.

probados: "…"Ha quedado probado que el acusado Basilio, mayor de edad, y sin antecedentes penales computables a efectos de reincidencia, quien mantuvo una relación sentimental durante un año con Concepción, con domicilio en Iruz (Santiurde de Toranzo), que cesó en julio de 2020, desde octubre de aquel año le llamaba por teléfono, envíaba mensajes de WhatsApp y cartas insistentemente, pidiéndole perdón y solicitándole retomar la relación diciendo "mi vida no tiene sentido, que estaba pensando cual era la mejor manera de desaparecer, que voy a hacer ahora, que la vida no tiene sentido para mí", habiéndole a las 09.00 horas del día 15 de diciembre encontrado sentado en una silla en su jardín seminconsciente con los ojos en blanco por lo que hubo de ser evacuado al hospital, acudiendo el día 1 de enero de 2021 a su domicilio llamando a la puerta, para posteriormente llamarle constantemente y remitirle una carta al mes, todo ello con la intención de alterar gravemente su vida, pese a tener conocimiento de que Concepción no quiere mantener ningún tipo de relación con él…"

La AP Sección 3ª de Santander, estimó el recurso de apelación del condenado al que absolvió, interponiendo la representación de la víctima recurso de casación que fue estimado, condenando de nuevo al acusado.

Fundamentos jurídicos.

Ante lo llamativo que resultan los pronunciamientos judiciales, condena en instancia, absolución en grado de apelación y de nuevo condena en vía casacional, la doctrina jurisprudencial del TEDH permite la revisión de sentencias absolutorias cuando el Tribunal Supremo actúa dentro de los márgenes de la infracción de ley, revisando cuestiones puramente jurídicas. Es decir, cuando esta Sala se limita a corregir errores de subsunción y a fijar criterios interpretativos uniformes para garantizar la seguridad jurídica, la predictibilidad de las resoluciones judiciales, la igualdad de los ciudadanos ante la ley penal, y la unidad del ordenamiento penal y procesal penal, sin alterar ningún presupuesto fáctico.

El art. 172.3 del Código Penal, vigente en el momento de comisión de los hechos -ya que el precepto ha sido reformado por la LO 1/2023 de 28 de febrero-, expresamente sanciona al " que acose a una persona llevando a cabo de forma insistente y reiterada, y sin estar legítimamente autorizado, alguna de las conductas siguientes y, de este modo, altere gravemente el desarrollo de su vida cotidiana". El citado artículo, que define el delito de acoso, se introdujo en el C. Penal en la L.O. 1/2015, de 30 de marzo, cuya Exposición de Motivos dispone que "se trata " de todos aquellos supuestos en los que, sin llegar a producirse necesariamente el anuncio explícito o no de la intención de causar algún mal (amenazas) o el empleo directo de violencia para coartar la libertad de la víctima (coacciones), se producen conductas reiteradas por medio de las cuales se menoscaba gravemente la libertad y sentimiento de seguridad de la víctima, a la que se somete a persecuciones o vigilancias constantes, llamadas reiteradas u otros actos continuos de hostigamiento".

En tales términos, se pronuncia la Jurisprudencia desde la Sentencia del Pleno 324/2017, de 8 de mayo, y la 554/2017, de 12 de julio, ésta última con expresa referencia a la anterior, donde se hace constar entre otras cosas que, por tanto, puede afirmarse que de forma insistente y reiterada equivale a decir que se está ante una reiteración de acciones de la misma naturaleza -- un continuum-- que se repite en el tiempo, en un periodo no concretado en el tipo penal, así como que se está en presencia de un tipo penal muy

"pegado" a los concretos perfiles y circunstancias del caso enjuiciado. Dicho de otro modo, el análisis de cada caso concreto, a la vista de las acciones desarrolladas por el agente con insistencia y reiteración, y por otra parte a la vista de la idoneidad de tales acciones para alterar gravemente la vida y tranquilidad de la víctima nos conducirá a la existencia o no de tal delito de acoso, correspondiendo a esta Sala de Casación, al descansar el recurso en la doble instancia --sentencia del Juez de lo Penal y sentencia de apelación dictada por la Audiencia Provincial-- determinar si dados los hechos probados existen o no los elementos que vertebran el delito.

Por otro lado, al margen de la definición legal, existen definiciones del fenómeno en la comunidad científica, básicamente en el ámbito de la psicología y la psiquiatría, en las que como regla general definen como comportamientos que un individuo inflige a otro mediante intrusiones o comunicaciones no deseadas, identificando la intrusión con el hecho de perseguir, merodear, cercar, vigilar, aproximarse, y comunicarse con conductas como enviar cartas, efectuar llamadas telefónicas, enviar e-mails, efectuar pintadas o notas en el coche, o conductas asociadas, como encargar servicios a nombre de la víctima, efectuar falsas acusaciones etc, exigiéndose siempre que esas conductas sean repetitivas o reiteradas.

El art. 172 ter, describe el tipo penal, con carácter general, empleando el verbo "acosar", término sobre el que no existe consenso en su definición en nuestro ordenamiento jurídico, sobre todo en cuanto la necesidad de cuantos actos son necesarios, pero, no podemos obviar que no requieren reiteración ni persistencia el acoso sexual y el acoso por razón de sexo, según el concepto de los mismos de los art. 7.1 y 7.2 de la Ley Orgánica 3/2007, de 22 de marzo, para la igualdad efectiva de las mujeres y los hombres, y la introducción en nuestro derecho penal del delito de stalking, es una respuesta más a la lucha contra la violencia de género y al cumplimiento de la normativa internacional y más específicamente del Convenio de Estambul.

También, hay que tener en cuenta, que el legislador, de forma acertada, según nuestro punto de vista, no determina el número de ocasiones que las conductas del hostigamiento deben producirse, ni el espacio temporal en que las mismas deben tener lugar, y en cuanto a la alteración grave de la vida cotidiana, hemos dicho que el tipo no exige planificación, pero sí una metódica secuencia de acciones que obligan a la víctima, como única vía de escapatoria, a variar, sus hábitos cotidianos. Para valorar esa idoneidad de la acción secuenciada para alterar los hábitos cotidianos de la víctima hay que atender al estándar del "hombre medio", aunque matizado por las circunstancias concretas de la víctima (vulnerabilidad, fragilidad psíquica, ...) que no pueden ser totalmente orilladas. (STS 639/2022, de 23 de junio).

Anticipamos, que el recurso ha de ser estimado, con la consiguiente anulación de la sentencia absolutoria y su sustitución por una sentencia de condena.

En el relato de hechos probados se describe la conducta del acusado, quien en un espacio temporal de al menos tres meses, llamó por teléfono en reiteradas ocasiones a su ex pareja, le envió mensajes de WhatsApp, y cartas, insistentemente dice el relato, en todos ellas pidiendo perdón y solicitando a la que fue su pareja sentimental retomar la relación que había cesado meses antes, diciendo "mi vida no tiene sentido, que estaba pensando cual era la mejor manera de desaparecer, que voy a hacer ahora, que la vida no tiene sentido para mí", incluso, un día la víctima se lo encontró sentado en una silla de su

jardín "semiinconsciente, con los ojos en blanco por lo que hubo de ser evacuado al hospital", acudiendo nuevamente 15 días después, al domicilio de Concepción llamando a la puerta, para después volver a llamarla por teléfono constantemente y remitirla una carta al mes, con la citada intención de retomar la relación pese a conocer que Concepción no quería mantener ningún tipo de relación con él.

El delito de acoso protege la libertad individual y el derecho a vivir tranquilo y sin zozobra. Los mensajes, aparición en el domicilio de la víctima mostrando su intento de suicidio para hacerla responsable a la misma de ello junto con las llamadas y mensajes enviados, son capaces por sí solos aptos para perturbar los hábitos, costumbres, rutinas o forma de vida de cualquier persona, atendido el estándar del 'hombre/mujer medio/a", reflejando el Juzgado Penal en su fundamentación que lo anterior obligó a la víctima a recibir apoyo psicológico, extremo no discutido. Los mismos actos de los hechos probados, -cubren las exigencias que esta Sala viene reclamando del tipo del art. 172 ter CP, a saber, insistencia, reiteración, repetición, reflejo de un mismo patrón o modelo sistemático, existencia de una voluntad de perseverar en esas acciones intrusivas, superando con creces lo puramente episódico o coyuntural y carencia de legitimación, o autorización para obrar de esa manera. Por el período de tiempo durante el cual se envían y por su contenido, el desvalor que encierran es de muy alta entidad, suficiente para activar la reacción penal.

En el supuesto, no estamos ante una simple conducta molesta, las acciones que se describen en el relato fáctico tienen idoneidad para alterar de cualquier manera la vida y tranquilidad de la víctima, una afectación o alteración en el devenir de la víctima de cualquier manera en su vida privada, laboral o relaciones con terceros. En definitiva, Concepción estaba sometida a un chantaje emocional, entendido como forma de comunicación que persigue la manipulación de una persona sobre otra haciendo uso del miedo, la obligación y especialmente, en este caso, la culpa.

Estamos ante unos hechos que implican una clara sumisión psicológica, en la que el acusado subyuga psicológicamente a su ex pareja bajo la traslación de la idea de que no parará hasta que vuelva con él, haciéndole incluso responsable de su propia vida con el intento autolítico en el jardín del domicilio de la víctima, lo que provoca en la misma temor, alterando gravemente su vida cotidiana, sometida a tratamiento psicológico, sin que sea necesario aportar al juicio una prueba pericial psicológica sobre la que se acredite la afectación a la psique de la víctima de esa situación de acoso o acecho, y que ello determine una alteración de su vida, cuando, como ocurre en este caso, se desprende del propio relato fáctico, pues los hechos, necesariamente, generaron en la víctima un impacto emocional -miedo por su seguridad y por la de su entorno- y un impacto en el normal desarrollo de su vida cotidiana, con necesidad de someterse a tratamiento psicológico.

Como hemos dicho en la STS 843/2021, de 4 de noviembre, la esencia del tipo penal, y, sobre todo, relacionado con hechos de violencia de género, como son los de acoso en situación de ex pareja, deben ser contemplados con perspectiva de género, ya que no es lo mismo una situación de acoso existente entre extraños, o conocidos, que en el vínculo de la relación de pareja, o ex pareja, en donde los lazos interpersonales que se han creado intensifican la situación de exigencias del acosador de dominación, o humillación, sobre la víctima que es, o ha sido, su pareja para conseguir la creación de unas ataduras físicas y psicológicas que evidencien esa sumisión que quiere trasladar el acosador sobre su víctima de que no se resista al acoso y vuelva con él.

En consecuencia, los hechos descritos son idóneos para obligar a la víctima a modificar su forma de vida, con entidad suficiente para constituir un delito de acoso de los tipificados en el artículo 172 ter del Código Penal, por tanto, procede estimar el recurso y condenar al acusado como autor del citado delito, a las mismas penas impuestas por el Juzgado de lo Penal, reponiendo la citada sentencia.

Conclusiones.

Importante precisión terminológica y fáctica de este tipo delictivo, que como bien dice la STS 295/2025, no cuantifica el número de actos de hostigamiento necesarios para integrar el tipo penal, pero que ambientalmente y valorando todos los indicios en su conjunto, no aisladamente, si permiten su apreciación porque la víctima vio alterada su forma de vida y más, en los casos de violencia sobre la mujer.

8.- STS 284/2025, de 27 de marzo. Abuso sexual sobre persona de 17 años con inteligencia límite. Daño moral.[8]

Antecedentes de hecho.

El Juzgado de lo Penal nº 6 de Las Palmas de Gran Canaria en la causa procedente del PA con el nº 247/2020, instruida por el Juzgado de Instrucción nº 1 de Telde, por un delito de abuso sexual contra Maximino dictó sentencia que contiene los siguientes Hechos Probados: "…ÚNICO.- Queda probado y así se declara que el encausado, Maximino, nacido en xx1984, el 1 de mayo de 2017 por la tarde, sin que pueda concretarse la hora, guiado del ánimo de satisfacer sus instintos sexuales, convenció a la menor de edad, 17 años, Socorro, a que le acompañara a la nave sita en la dirección xxx, y una vez allí, le realizó tocamientos en las nalgas, y en el muslo, aprovechándose, y a sabiendas de que era menor y de que ésta presentaba un nivel de funcionamiento intelectual en el límite con la inteligencia normal, presentando una alta vulnerabilidad para ser víctima de hechos. La legítima representante de la menor reclama…"

En grado de apelación la Audiencia Provincial estimó parcialmente el recurso por dilaciones indebidas y la STS confirmó el fallo condenatorio de la Audiencia Provincial.

Fundamentos jurídicos.

Postula el recurrente por un lado, la atipicidad de los hechos basándose en la concurrencia de consentimiento de la víctima. La descripción del hecho no permitiría fundar un abuso de trastorno mental. La sentencia habla de un nivel de funcionamiento intelectual en el límite con la inteligencia normal. Al estar en el límite y no por debajo del límite -se enfatiza tipográficamente- no podría hablarse de abuso de trastorno.

La argumentación no se capta de forma clara. Por un lado, parece que se está razonando que el acusado no conocía esa circunstancia. Eso contradice el hecho probado

[8] STS 284/2025, Penal Sección 1ª, de 27 de marzo publicada en la web del CGPJ, Centro de Documentación Judicial, CENDOJ. (ROJ: STS 1469/2025 - ECLI:ES:TS:2025:1469), recurso: 7022/2022. Ponente Excmo. Sr. D. Antonio del Moral García.

que le atribuye un aprovechamiento de esa característica, lo que implica conocimiento. Se convierte así en inviable la pretensión.

También podría querer expresarse que, estando en el límite de la normalidad, podría hablarse de normalidad lo que privaría de sustento a la ausencia de consentimiento.

Este segundo eventual argumento juega con el lenguaje, ignorando que las locuciones, inteligencia límite o funcionamiento intelectual límite, constituyen conceptos bien acuñados que expresan algo más de lo que se derivaría de su estricta literalidad. Las personas con esas características carecen de lo que se considera un nivel intelectual medio. Son -y esto pertenece al acervo cultural común: no se trata de tecnicismos psiquiátricos y, mucho menos, jurídicos- personas capaces de desarrollar procesos de vida, desenvolverse y comprender el mundo, pero precisan de apoyos adecuados, en tanto su bajo coeficiente intelectual los reclama. Presentan dificultades para la toma de decisiones, y en la resolución de conflictos; sus habilidades sociales aparecen disminuidas. La Organización Mundial de la Salud establece que la inteligencia media se mueve en un coeficiente intelectual entre el 85 y el 115. Pues bien, las personas con inteligencia límite son las que están justo por debajo de esas cifras: entre el 70 y el 85. No se puede hablar sanitariamente de discapacidad intelectual, pero están cercanos a esa frontera. Como tampoco se puede hablar de normalidad intelectual. Desde una perspectiva jurídico penal sí queden abarcados en el concepto normativo del art. 25.1 CP.

Los hechos probados, por lo demás, como luego aclara más aún algún pasaje de la motivación fáctica, no mencionan ningún consentimiento de la menor respecto de los tocamientos con implicaciones sexuales. No se dice que los aceptase. Le fueron impuestos hasta que logró zafarse, aunque sin empleo de violencia ni intimidación. De hecho, la sentencia no cita el art. 181.2 (abuso de trastorno mental).

La realización de actos sexuales sin contar con el consentimiento de la otra persona es típica por sí misma, con independencia de cuál sea el nivel intelectual de la víctima. Si, además, ésta presenta unos déficits intelectuales determinantes de una especial vulnerabilidad, el hecho merecerá una agravación.

Y es que la segunda línea impugnativa del recurso trata de expulsar esa agravación considerándola inherente al abuso de un trastorno mental o ajena al conocimiento del acusado.

Solo retorciendo el hecho probado se puede sostener que el acusado no conocía esa especial vulnerabilidad que dimana de esa inteligencia límite de la que se aprovecha. Por lo demás, la secuencia de los hechos y la forma en que estos se recrean en la fundamentación jurídica, son tremendamente expresivos.

Si se tratase de un supuesto en que se obtiene la anuencia, expresa o exteriorizada por actos concluyentes, de la víctima, y el carácter típico se fundase en enfrentarnos a un consentimiento no libre por ausencia de capacidad para otorgarlo y con aprovechamiento del autor del déficit cognitivo para arrancarlo, surgiría el problema de la compatibilidad del art. 181.2 anterior (abuso de trastorno mental) o del art. 178.2 vigente (abuso de una situación de vulnerabilidad de la víctima) con la agravación específica (especialmente vulnerable por razón... de su edad, enfermedad, discapacidad o situación: art. 180.1.3º y 181.5 en la legislación aplicada; o especial vulnerabilidad por razón... de su

discapacidad o por cualquier otra circunstancia: art. 180.1.3º tras la LO 10/2022). Pero no es el caso.

De un lado, se constata ausencia de consentimiento. No estamos ante un consentimiento no libre por haber sido obtenido abusivamente. Y de otro lado, aparece que la víctima presenta una disminuida capacidad intelectual que la convierte en especialmente vulnerable.

La tipificación por lo tanto ha sido correcta.

Y lo que destaca a continuación de la STS es el concepto y alcance del daño moral, que tanto cuesta ver en la práctica diaria de nuestros tribunales.

Tan es así que el art. 193 CP contiene una prescripción, en las sentencias condenatorias por delitos contra la libertad sexual, además del pronunciamiento correspondientes a la responsabilidad civil, se harán, en su caso, los que procedan en orden a la filiación y fijación de alimentos, que viene a representar una presunción legal (basada en una máxima de experiencia compartida e indubitada) de daños morales en este tipo de delitos (vid SSTS 327/2013, de 4 de marzo; 1033/2013, de 26 de octubre; 733/2016, de 5 de octubre; 812/2017, de 11 de diciembre; 393/2020, de 15 de julio; 1040/2021, de 26 de octubre ó 1209/2021, de 2 de diciembre).

También en la jurisdicción civil -no lo dude el recurrente- se acordaría una indemnización si se hubiese reservado la acción para ese ámbito.

Aunque no es norma aplicable por no estar vigente en el momento de los hechos, resulta pertinente aludir a la regulación de esta cuestión en Ley Orgánica 10/2022, de 6 de septiembre, de garantía integral de la libertad sexual, en tanto viene a refrendar, con novedosos aditamentos, la inexcusabilidad de esa indemnización desglosando conceptos en los que aparece destacado el daño moral y a la dignidad.

Reza así el art. 53 de la citada Ley, bajo el acápite Indemnización.

"1. La indemnización por daños y perjuicios materiales y morales que corresponda a las víctimas de violencias sexuales de acuerdo con las leyes penales sobre la responsabilidad civil derivada del delito, deberá garantizar la satisfacción económicamente evaluable de, al menos, los siguientes conceptos:

a) El daño físico y psicológico, incluido el daño moral y el daño a la dignidad.

b) La pérdida de oportunidades, incluidas las oportunidades de educación, empleo y prestaciones sociales.

c) Los daños materiales y la pérdida de ingresos, incluido el lucro cesante.

d) El daño social, entendido como el daño al proyecto de vida.

e) El tratamiento terapéutico, social y de salud sexual y reproductiva.

2. La indemnización será satisfecha por la o las personas civil o penalmente responsables, de acuerdo con la normativa vigente"

Conclusiones.

Dos cuestiones de interés, aborda esta STS 284/2025. De un lado el perfecto encaje de una figura agravada en delitos contra la liberta sexual, cuando ha habido un desvalor de la acción del agresor que no sólo es objetiva, actos de tocamiento, sino que también tiene una relevante perspectiva subjetiva, el aprovechamiento de la vulnerabilidad de la víctima, a sabiendas. De otro, ese concepto casi olvidado del daño moral, que aunque existente con anterioridad en numerosos pronunciamientos judiciales, ha tenido su expreso reconocimiento en la controvertida LO 10/2022 de garantía integral de la libertad sexual.

GOBIERNO DE ESPAÑA
MINISTERIO DEL INTERIOR
GUARDIA CIVIL

Revista Científica
del Centro Universitario de la Guardia Civil

Revista Lógos Guardia Civil

CENTRO UNIVERSITARIO GUARDIA CIVIL