# INTELIGENCIA Y TOMA DE DECISIONES: PERSPECTIVAS ACTUALES

Dirección
**Diego González López**

COLEX READER | COLEX AUDIO
NEDSE
COLEX

**¡Gracias por confiar en nosotros!**

La obra que acaba de adquirir incluye de forma gratuita la versión electrónica. Acceda a nuestra página web para aprovechar todas las funcionalidades de las que dispone en nuestro lector.

# Funcionalidades eBook

**Acceso desde cualquier dispositivo con conexión a internet**

**Idéntica visualización a la edición de papel**

**Navegación intuitiva**

**Tamaño del texto adaptable**

Síguenos en:

# 1

# INTELIGENCIA Y TOMA DE DECISIONES

PERSPECTIVAS ACTUALES

# INTELIGENCIA, DEFENSA Y SEGURIDAD




La presente obra ha sido evaluada externamente bajo el sistema de revisión por pares en modalidad anónima, y se encuentra respaldada por el Consejo Editorial.

La presente obra ha sido dirigida por Diego González López, beneficiario de la subvención para la contratación de personal docente e investigador predoctoral (Universidad de Valencia) ACIF de la Generalitat Valenciana y Vocal académico de INDESEC.

La presente obra ha sido financiada por la Asociación de Jóvenes en Inteligencia, Defensa y Seguridad (INDESEC) como parte de su actividad.

# 1

# INTELIGENCIA Y TOMA DE DECISIONES

## PERSPECTIVAS ACTUALES

Dirección
**Diego González López**

COLEX 2025



© Editorial Colex, S.L.
Calle Costa Rica, número 5, 3.º B (local comercial)
A Coruña, 15004, A Coruña (Galicia)
info@colex.es
www.colex.es

# SUMARIO

Prólogo ..... 17

**EL ANALISTA DE INTELIGENCIA 4.0**

*Joaquín González López*

1. Introducción: ¿Un nuevo paradigma en la inteligencia? ..... 19
2. El ecosistema de la información en la era digital: desafíos y oportunidades ... 22
3. La adopción de tecnologías emergentes: big data, IA y computación ..... 24
4. La gestión del riesgo y la incertidumbre en la toma de decisiones ..... 26
5. La nueva filosofía de producción analítica ..... 28
6. Ética y gobernanza de la inteligencia digital ..... 29
7. El perfil y las competencias del analista 4.0. ..... 32
8. Conclusiones ..... 36

BIBLIOGRAFÍA. ..... 37

**LA ÉTICA COMO EJE TRANSVERSAL EN LA INTELIGENCIA**

*Andrea Andreu Gutiérrez*

1. Introducción ..... 39
2. El concepto de inteligencia y su dimensión ética. ..... 42
3. Principios rectores de las actividades de inteligencia ..... 46
4. Jurisprudencia relevante en la materia. ..... 50
5. Conclusiones ..... 52

BIBLIOGRAFÍA. ..... 53

**ÉTICA, AUTONOMÍA Y OPERATIVIDAD EN INTELIGENCIA: FUNAMBULISMO EN LA ZONA GRIS**

*Alejandro López Palma*

1. Introducción ..... 55
2. La inteligencia y su evolución ética. ..... 57
3. Confidence Building Measures (CBM): ética y política de la confianza. ..... 60
   3.1. Origen y fundamentos conceptuales. ..... 60
   3.2. Aplicación al campo de la inteligencia ..... 61

3.3. Dilemas éticos, políticos y operativos . . . . . 62
3.4. Potencial de futuro . . . . . 63
4. Autonomía operativa vs. control democrático: una tensión estructural . . . . . 64
4.1. La autonomía como condición funcional de la inteligencia . . . . . 64
4.2. Riesgos institucionales y precedentes históricos . . . . . 64
4.3. Consecuencias políticas y sociales de los abusos . . . . . 65
4.4. Dificultades estructurales del control democrático . . . . . 66
4.5. Modelos de supervisión: entre el ideal y lo posible . . . . . 66
5. Modelos híbridos de supervisión: hacia un equilibrio sostenible . . . . . 67
5.1. Supervisión interna especializada . . . . . 67
5.2. Comisiones parlamentarias reducidas y profesionalizadas . . . . . 68
5.3. Revisión judicial segmentada y técnica . . . . . 68
5.4. Auditorías externas y contralorías técnicas . . . . . 69
5.5. Publicación de informes desclasificados . . . . . 69
5.6. Nombramientos, mandatos y garantías institucionales . . . . . 70
6. Perspectivas futuras y desafíos . . . . . 70
7. Conclusiones . . . . . 72
BIBLIOGRAFÍA . . . . . 73

**DE LA LEY DE SECRETOS OFICIALES DE 1968 A LA NUEVA LEY DE INFORMACIÓN CLASIFICADA DE 2025**

*César Augusto Giner Alegría*
*Patrick Salvador Peris*

1. Introducción . . . . . 75
2. Antecedentes normativos . . . . . 76
2.1. La Ley de Secretos Oficiales de 1968 . . . . . 76
2.2. Reformas fallidas previas . . . . . 77
2.3. Exigencias internacionales y derecho comparado . . . . . 78
3. El Anteproyecto de Ley de Información Clasificada de 2025 . . . . . 80
3.1. Estructura y principios generales . . . . . 80
3.2. Categorías de clasificación . . . . . 81
3.3. Plazos de desclasificación . . . . . 82
3.4. Autoridades competentes . . . . . 83
3.5. Procedimiento de clasificación y desclasificación . . . . . 85
3.6. Régimen sancionador . . . . . 86
4. Transparencia y acceso a la información . . . . . 87
4.1. Derecho de acceso de periodistas, historiadores y ciudadanos . . . . . 87
4.2. Límites: seguridad nacional vs. derecho a la información . . . . . 88
4.3. Excepciones: violaciones graves de derechos humanos y crímenes de lesa humanidad . . . . . 89
5. Perspectiva comparada: Colombia y Bélgica . . . . . 89

6. Conclusiones . . . . . 92
BIBLIOGRAFÍA . . . . . 94

## EL CONTROL DE LOS GASTOS RESERVADOS DEL CNI: ANÁLISIS JURÍDICO-PENAL A LA LUZ DE LA LEY 11/1995

*Carlos Álvaro Peris*

1. Introducción . . . . . 97
2. El conflicto entre el derecho a la libre información y la seguridad y defensa del estado . . . . . 98
3. Marco jurídico-normativo . . . . . 100
3.1. Autonomía del CNI . . . . . 101
3.2. Concepto y naturaleza de los gastos reservados . . . . . 102
3.3. Control administrativo . . . . . 103
3.4. Control parlamentario . . . . . 105
4. Posible comisión de delitos de malversación ante una incorrecta gestión de los gastos reservados . . . . . 109
5. Conclusiones . . . . . 114
BIBLIOGRAFÍA . . . . . 116

## INTELIGENCIA ECONÓMICA Y SEGURIDAD ENERGÉTICA EN LA CULTURA DE SEGURIDAD Y DEFENSA

*Alberto Camarero Orive*

1. Introducción . . . . . 119
2. Evolución de la inteligencia económica aplicada a la seguridad energética . . . 120
3. El nuevo paradigma de la seguridad energética y su relación con la inteligencia económica . . . . . 121
4. Diversificación estratégica, resiliencia y gestión de vulnerabilidades . . . . . 122
5. Nuevas fuentes de energía y retos tecnológicos . . . . . 123
6. Cultura de seguridad y defensa: formación, cooperación y gobernanza . . . . . 124
7. Acciones y propuestas estratégicas para España y la UE . . . . . 125
8. Perspectivas futuras y conclusiones . . . . . 126
BIBLIOGRAFÍA . . . . . 127

## LA ACTUACIÓN DE LOS SERVICIOS DE INTELIGENCIA EN LA PROTECCIÓN DEL MEDIOAMBIENTE

*Alejandra Moreno García*

1. Introducción . . . . . 129
2. El crimen medioambiental en la Unión Europea . . . . . 130
2.1. Conceptualización y tipologías . . . . . 130
2.2. Factores de crecimiento del crimen medioambiental y motivaciones . . . . . 132

2.3. Impacto ecológico, social y económico ..... 133
3. La seguridad ambiental y los servicios de inteligencia ..... 135
3.1. Servicios de inteligencia: actores clave en la lucha contra el crimen medioambiental ..... 135
3.2. La dimensión estratégica de la seguridad ambiental ..... 136
3.3. Operaciones relevantes en la lucha contra la delincuencia medioambiental ..... 137
3.4. Inteligencia y retos frente a la delincuencia ambiental ..... 138
4. Herramientas para la inteligencia ambiental ..... 140
4.1. Proyecto EMERITUS ..... 141
4.2. Proyecto GIEDA: inteligencia geoespacial para la evaluación de daños ambientales ..... 141
5. Propuesta de un modelo estratégico para la inteligencia ambiental en la Unión Europea ..... 142
6. Conclusiones ..... 144
BIBLIOGRAFÍA ..... 145

**LA RADICALIZACIÓN EN PRISIONES COMO DESAFÍO PARA LOS SERVICIOS DE INTELIGENCIA**

*Susana Berrocal Díaz*

1. Introducción ..... 147
2. Análisis de la problemática: la realidad de la radicalización yihadista en prisiones ..... 148
2.1. Factores de riesgo en los centros penitenciarios: una visión general ..... 150
2.2. Situación en las prisiones españolas ..... 152
3. La ENCOT 23-24 y el entorno penitenciario ..... 154
4. Inteligencia penitenciaria: detección y seguimiento ..... 157
5. Conclusiones ..... 160
BIBLIOGRAFÍA ..... 162

**DEL INFORME DRAGHI (O LA BRÚJULA PARA LA COMPETITIVIDAD) A LA ACCIÓN: ¿UNA DIVISIÓN DE INTELIGENCIA ECONÓMICA EN LA COMISIÓN EUROPEA?**

*Diego González López*

1. Introducción ..... 165
2. Consideraciones previas ..... 167
2.1. El sistema competencial de la Unión Europea ..... 167
2.2. La Comisión Europea ..... 168
2.3. La estructura de inteligencia europea ..... 169
2.4. Inteligencia competitiva vs. inteligencia económica ..... 171
2.5. El Informe Draghi: ¿una última llamada? ..... 172
3. Propuesta: una División de Inteligencia Económica ..... 174

4. Propuesta alternativa: transformar el Joint Research Centre ..... 175
5. Conclusiones ..... 176
BIBLIOGRAFÍA ..... 177

**DESAFÍOS POLÍTICOS Y JURÍDICOS PARA UNA COMUNIDAD DE INTELIGENCIA EUROPEA: ENTRE SEGURIDAD Y PROTECCIÓN DE DATOS**

*Irene Gil Matos*

1. Introducción ..... 179
2. Marco jurídico general de la seguridad y la protección de datos en la unión europea ..... 181
3. Desarrollo y actualidad de las dinámicas de cooperación europeas ..... 184
4. La tensión entre la seguridad y la protección de derechos humanos ..... 186
5. Obstáculos para una comunidad de inteligencia integrada ..... 190
6. Conclusiones ..... 192
BIBLIOGRAFÍA ..... 194

**LA IMPORTANCIA DE LA COMUNICACIÓN EN LA INTELIGENCIA ESTRATÉGICA**

*Inmaculada Crespo González*
*Patricia Pérez Rodríguez*

1. Introducción ..... 197
2. Definición y fundamentos de la inteligencia estratégica ..... 199
3. Fase de difusión en el ciclo de inteligencia: cómo aplicar la inteligencia narrativa ..... 203
3.1. ¿Qué es la inteligencia narrativa? ..... 203
3.2. Por qué la comunicación efectiva es decisiva en inteligencia ..... 203
3.3. Storytelling y valor explicativo en informes estratégicos ..... 204
3.4. Ejemplo CHALLENGER: cuando la narrativa falla ..... 204
3.5. Subrayado final: comunicar bien es parte de «pensar bien» ..... 205
4. Modelos de narrativas estructuradas en inteligencia ..... 205
4.1. Pirámide invertida ..... 206
4.2. Narrativa persuasiva ..... 206
4.3. Escenarios hipotéticos ..... 206
4.4. Narrativas colaborativas y micro-narrativas ..... 207
5. Formación del analista para la redacción de informes estratégicos ..... 207
5.1. Dimensiones de formación para el analista ..... 208
5.2. Avance de las herramientas para la redacción de informes ..... 208
5.3. Ejemplo práctico: construcción de un informe narrativo ..... 209
5.4. Consideraciones finales ..... 210
6. Conclusión ..... 211
BIBLIOGRAFÍA ..... 212

## LA COMUNICACIÓN ESTRATÉGICA Y EL LENGUAJE SOBRE DEFENSA, SEGURIDAD E INTELIGENCIA: ANÁLISIS DE CASOS EN ESPAÑA

*Raquel Pinilla Gómez*

1. Introducción ..... 215
2. Conceptos clave en el ámbito de la defensa, la seguridad y la inteligencia. ..... 217
2.1. Defensa, seguridad e inteligencia ..... 218
2.2. Cultura de defensa y cultura de inteligencia. ..... 219
2.3. Fuerzas Armadas ..... 220
3. Retos de la comunicación estratégica sobre defensa, seguridad e inteligencia . 221
3.1. El fenómeno de la desinformación ..... 224
4. La comunicación y el lenguaje de las instituciones de defensa, seguridad e inteligencia: CESEDEN, DSN y CNI. ..... 225
4.1. El Centro Superior de Estudios de la Defensa Nacional (CESEDEN) ..... 226
4.2. El Departamento de Seguridad Nacional (DSN) ..... 227
4.3. El Centro Nacional de Inteligencia (CNI) ..... 229
5. Conclusiones ..... 230
BIBLIOGRAFÍA. ..... 231

## VENTAJAS E INCONVENIENTES EN EL USO DE FUENTES PARA EL ANÁLISIS DE LA PIRATERÍA MARÍTIMA

*Fernando Ibáñez Gómez*

1. Introducción ..... 233
2. Una definición de piratería no siempre compartida ..... 234
3. Fuentes para el análisis de la piratería marítima ..... 235
3.1. Centros globales de carácter público ..... 235
3.1.1. International Maritime Organization. ..... 235
3.1.2. Maritime Information Cooperation & Awareness Center. ..... 236
3.2. Centros globales de carácter privado. ..... 237
3.2.1. International Maritime Bureau Piracy Reporting Center ..... 237
3.2.2. Consultoras de seguridad privada ..... 238
3.3. Centros regionales de carácter público. ..... 239
3.3.1. United Kingdom Marine Trade Operations. ..... 239
3.3.2. Maritime Security Centre-Horn of Africa y Maritime Security Centre Indian Ocean ..... 240
3.3.3. Maritime Domain Awareness for Trade-Gulf of Guinea ..... 242
3.3.4. The Regional Cooperation Agreement on Combating Piracy and Armed Robbery against Ships in Asia. ..... 243
3.4. Centros que aportan información complementaria ..... 244
3.4.1. The Information Fusion Center ..... 244
3.4.2. Information Fusion Centre-Indian Ocean Region ..... 244
3.4.3. Office of Naval Intelligence ..... 245
4. Análisis comparativo de las distintas fuentes. ..... 245

5. Conclusiones . . . . . 248
BIBLIOGRAFÍA . . . . . 249

**PERSPECTIVAS ACTUALES Y FUTURAS DE LOS MÉTODOS DE OBTENCIÓN DE INFORMACIÓN DE LOS SERVICIOS DE INTELIGENCIA PORTUGUESES: LAS INTERCEPTACIONES TELEFÓNICAS Y LOS DATOS DE TRÁFICO**

*João Miguel Oliveira Narciso*

1. Introducción . . . . . 251
2. El sistema de información de la República Portuguesa . . . . . 252
3. Los medios de obtención de información de los servicios de inteligencia portugueses: situación actual . . . . . 256
3.1. El problema del acceso a los datos de tráfico . . . . . 259
3.1.1. El ámbito de protección del derecho al secreto de las telecomunicaciones . . . . . 259
3.2. La cuestión de la inclusión de la inteligencia en el ámbito de la «materia de proceso criminal» . . . . . 261
4. Perspectivas futuras . . . . . 263
5. Conclusiones . . . . . 266
BIBLIOGRAFÍA . . . . . 267

**EL SISTEMA ESPAÑOL DE INTELIGENCIA FINANCIERA PARA COMBATIR EL BLANQUEO DE CAPITALES**

*Yago González Quinzán*

1. Introducción . . . . . 269
2. La inteligencia financiera en el marco de la inteligencia económica: estado de la disciplina en España . . . . . 271
3. La Comisión de Prevención del Blanqueo de Capitales e Infracciones Monetarias . . . . . 273
3.1. El Pleno de la Comisión . . . . . 274
3.2. El Comité Permanente de la Comisión . . . . . 275
3.3. El Comité de Inteligencia Financiera . . . . . 276
4. Los órganos de apoyo de la Comisión de Prevención del Blanqueo de Capitales e Infracciones Monetarias . . . . . 277
4.1. La Secretaría de la Comisión . . . . . 277
4.2. El SEPBLAC como UIF nacional . . . . . 278
4.2.1. La demanda de creación por la normativa internacional . . . . . 278
4.2.2. El intercambio de información financiera en la Unión Europea . . . . . 279
4.2.3. El Grupo Egmont para el intercambio de información financiera . . . . . 281
4.2.4. Régimen y estructura . . . . . 283
4.2.5. Atribuciones . . . . . 285
5. A modo de recapitulación . . . . . 289
BIBLIOGRAFÍA . . . . . 290

## EL PAPEL DEL SEPBLAC COMO UNIDAD DE INTELIGENCIA FINANCIERA EN LA LUCHA CONTRA EL FRAUDE FISCAL Y EL BLANQUEO DE CAPITALES

*Raquel Alamà Perales*

1. Introducción ..... 293
2. El origen de las UIF en el contexto de internacional ..... 295
2.1. La Convención de Viena de 1988 y el origen de la cooperación global en blanqueo de capitales..... 295
2.2. El GAFI y sus 40 Recomendaciones ..... 297
2.3. El Grupo Egmont y la red mundial de UIF ..... 299
2.4. Modelos comparados de UIF: administrativo, policial, judicial e híbrido .. 302
2.4.1. UIF administrativa ..... 302
2.4.2. UIF policial ..... 303
2.4.3. UIF judicial ..... 303
2.4.4. UIF híbrida ..... 304
2.4.5. Consideraciones transversales de diseño ..... 304
3. El Servicio Ejecutivo de la Comisión de Prevención del Blanqueo de Capitales e Infracciones Monetarias ..... 305
3.1. Naturaleza y funciones ..... 306
3.1.1. Recepción, análisis y difusión de información financiera..... 306
3.1.2. Supervisión de sujetos obligados..... 307
3.1.3. Cooperación nacional e internacional ..... 307
4. La cooperación del SEPBLAC con la Agencia Estatal de la Administración Tributaria ..... 308
5. Conclusiones ..... 310
BIBLIOGRAFÍA..... 311

## EL IMPACTO DE LA INTELIGENCIA ARTIFICIAL Y LA AUTOMATIZACIÓN DE DATOS EN LA TOMA DE DECISIONES EN EL SECTOR PÚBLICO

*Blanca Aparicio Araque*

1. Introducción ..... 313
2. La inteligencia artificial..... 314
2.1. Concepto ..... 314
2.2. Características principales..... 316
2.3. Los datos y la inteligencia artificial ..... 317
3. Regulación de la inteligencia artificial..... 318
3.1. El Reglamento de IA: sistemas de alto riesgo ..... 318
3.2. Las propuestas del Grupo de Trabajo del CGPJ sobre tecnología, inteligencia artificial y justicia ..... 319
4. El impacto de la inteligencia artificial en las decisiones automatizadas ..... 320
4.1. El impacto en el sector judicial..... 320
4.1.1. Aplicación asistencial o instrumental ..... 322
4.1.2. Aplicación cautelar ..... 323

4.1.3. Aplicación de ayuda a la decisión automatizada ..... 324
4.1.4. Aplicación de justicia robotizada ..... 324
4.1.5. La digitalización de la justicia en América Latina ..... 325
4.2. El impacto en el sector defensa ..... 326
4.2.1. La inteligencia artificial en la toma de decisiones estratégicas ..... 327
4.2.2. La inteligencia artificial en el contexto armamentístico y de misiones militares ..... 328
5. Desafíos emergentes de la inteligencia artificial ..... 329
6. Responsabilidad civil derivada de un posible daño ..... 330
7. Conclusiones ..... 332
BIBLIOGRAFÍA ..... 333

**MATRIZ IC-IP: UNA HERRAMIENTA PARA APOYAR LA PROSPECTIVA ELECTORAL EN EMPRESAS INTERNACIONALIZADAS**

*Pablo Las Heras*

1. Introducción ..... 337
2. Marco teórico y conceptual ..... 339
2.1. Prospectiva y anticipación estratégica ..... 339
2.2. Inteligencia aplicada y técnicas estructuradas ..... 339
2.3. Análisis político, sistemas electorales y efecto empresa ..... 340
3. Metodología propuesta ..... 341
3.1. Fase 1: Análisis de contexto ..... 341
3.2. Fase 2: Análisis de posición ..... 342
3.3. Fase 3: Integración. Matriz contexto-posición ..... 343
3.4. Fase 4: Culminación. Generación de escenarios ..... 345
4. Ventajas y límites ..... 345
4.1. Ventajas y fortalezas ..... 346
4.2. Límites y advertencias ..... 346
4.3. Recomendaciones de uso ..... 347
5. Conclusiones ..... 349
BIBLIOGRAFÍA ..... 350

Epílogo ..... 351

# PRÓLOGO

Es para mí motivo de satisfacción presentar la obra colectiva *Inteligencia y toma de decisiones: perspectivas actuales*, dirigida por Diego González López y editada por Colex. La misma reúne a un grupo de destacados especialistas con el propósito de reflexionar sobre el papel de la inteligencia en los procesos de decisión en el mundo contemporáneo. El lector tiene en sus manos un trabajo riguroso y plural que se adentra en una de las cuestiones más decisivas de nuestro tiempo: cómo afrontar la creciente complejidad de las sociedades actuales a través de instrumentos que permitan interpretar la realidad y orientar la acción con criterios de eficacia, legalidad y legitimidad.

Vivimos en un contexto marcado por la incertidumbre, la aceleración de los cambios tecnológicos, la interdependencia global y la emergencia de riesgos y amenazas que trascienden fronteras y disciplinas. En este escenario, la inteligencia no puede entenderse como una actividad periférica o reservada a ámbitos estrictamente securitarios. Al contrario, se ha convertido en un recurso estratégico imprescindible, tanto en el sector público como en el privado, para comprender los problemas, anticipar tendencias y diseñar respuestas proporcionadas. La toma de decisiones responsable exige hoy disponer de sistemas de inteligencia sólidos, capaces de integrar información diversa, de analizarla con rigor y de proyectar escenarios plausibles.

La obra que aquí se presenta tiene precisamente esa virtud: ofrecer una visión amplia y multidisciplinar de la inteligencia como disciplina al servicio de la toma de decisiones. A través de sus capítulos, se recorren ámbitos muy diversos que ilustran la riqueza y complejidad de este campo. Así, encontramos estudios dedicados al perfil y las competencias del analista de inteligencia en la era digital, al impacto ético de la actividad de inteligencia, a la necesaria regulación jurídica en torno a la información clasificada o al control de los gastos reservados. Otros trabajos abordan desafíos emergentes como la protección del medio ambiente, la radicalización en las prisiones o la comunicación estratégica en materia de seguridad y defensa. Asimismo, el libro se adentra en la inteligencia financiera, en los métodos de obtención de información en contextos nacionales y europeos, en la importancia de la narrativa en los informes estratégicos, en la lucha contra la piratería marítima o en la prospectiva electoral aplicada a la empresa internacionalizada. Y no podía faltar un análisis específico sobre la inteligencia artificial y sus repercusiones en la toma de decisiones, cuestión de máxima actualidad y trascendencia.

El lector advertirá que no se trata únicamente de una suma de capítulos, sino de un proyecto intelectual coherente, que combina reflexión teórica, análisis normativo y estudio de casos. Cada aportación ilumina una dimensión distinta del fenómeno, pero todas ellas convergen en un punto común: la convicción de que la inteligencia debe desarrollarse bajo parámetros de legalidad, ética y responsabilidad social, al tiempo que se adapta a las transformaciones tecnológicas y geopolíticas de nuestro tiempo. Esa complementariedad entre el rigor académico y la atención a las aplicaciones prácticas confiere al libro un valor especial, tanto para investigadores y docentes como para profesionales de la seguridad, responsables institucionales y analistas de inteligencia.

No quisiera dejar de subrayar el esfuerzo colectivo que subyace a este volumen. Coordinar miradas tan variadas no es tarea sencilla, y sin embargo el resultado es un libro que logra ofrecer al lector una panorámica completa y bien articulada. Se percibe en sus páginas la dedicación de los autores, la solidez de sus trayectorias y la voluntad común de contribuir a una mejor comprensión de los retos que enfrentamos.

Confío en que esta obra no solo aporte conocimiento, sino que también invite a nuevas investigaciones, fomente el debate académico y ayude a mejorar las prácticas profesionales en un terreno tan decisivo como es la inteligencia aplicada a la toma de decisiones. Estoy convencido de que las reflexiones contenidas en estas páginas se convertirán en un referente útil para quienes deseen comprender, desde distintas perspectivas, cómo se construyen las decisiones en escenarios marcados por la volatilidad, la incertidumbre y la complejidad.

Con estas palabras presento al lector un libro que, sin duda, merece ser leído con atención. Mi agradecimiento más sincero a todos los autores que han hecho posible este proyecto (especialmente a su director) y a la editorial Colex, y mi deseo de que sus contribuciones inspiren nuevas formas de pensar y de actuar en beneficio de nuestras sociedades.

Valencia, septiembre de 2025.

**José León Alapont**

*Profesor Titular de Derecho Penal*
*Universidad de Valencia*

# EL ANALISTA DE INTELIGENCIA 4.0

**Joaquín González López**
*Director del Departamento de Inteligencia en Grupo FCC*

## 1. Introducción: ¿Un nuevo paradigma en la inteligencia?

El entorno global contemporáneo, marcado por la hiperconectividad y una acelerada revolución tecnológica sin límites, ha forzado una redefinición fundamental del papel y las metodologías del analista de inteligencia. La transformación digital y la consolidación de la Inteligencia Artificial (en adelante también IA) no son simplemente herramientas adicionales para este oficio ancestral de la producción de inteligencia; por el contrario, actúan como catalizadores de una transformación radical que impulsa un nuevo modelo de elaboración de inteligencia (producción)[1]. Este cambio desplaza el enfoque tradicional, a menudo reactivo y centrado en la simple acumulación de secretos, hacia un proceso proactivo, analítico y, crucialmente, centrado en el usuario final[2].

Este documento explora la necesidad, las características distintivas y los desafíos que definen a este nuevo perfil profesional, denominado Analista de Inteligencia 4.0, por formar parte de este momento histórico de la cuarta revolución industrial, denominado también de la Industria 4.0, como sinónimo de fabricación inteligente: más productiva, flexible y ágil a partir de decisiones en tiempo real, gracias al aumento de la automatización y el empleo de máquinas y fábricas inteligentes.

El término «Analista de Inteligencia 4.0» encapsula al profesional de la inteligencia que opera de manera efectiva en estos entornos actuales que se han dado en definir como: Volátiles, Inciertos, Complejos, Ambiguos (VUCA)[3]; Frágiles, que generan Ansiedad, No Lineales, Incomprensibles (BANI) o de

1. Pherson, R. H., Arcos, R., *Intelligence communication in the digital era: Transforming security, defence and business*, Palgrave Macmillan, Basingstoke, 2015, pág. 2.

2. Véase Stenslie, S., Haugom, L., Vaage, B. H., *Intelligence analysis in the digital age,* Routledge, Abingdon, 2021.

3. Páramo, A., «El analista de inteligencia de última generación», en Arteaga, F., Ríos Insúa, D. (coords.): *El analista de inteligencia en la era digital*, Real Instituto Elcano, Centro Nacional de Inteligencia, 2022, pág. 21.

tiempos *postnormales*[4]. Su rol supera los límites del ciclo de inteligencia convencional para concentrarse en la creación de valor, la comunicación de impacto y la colaboración con sistemas inteligentes[5]. A diferencia de sus predecesores, el analista 4.0 se distingue por su capacidad para integrar conocimientos de diversas disciplinas, desde la geopolítica hasta la computación, y por su enfoque en la anticipación y la proactividad, ya que esta transformación digital también ha incrementado la exposición al riesgo, especialmente para los activos digitales, ha influido en la percepción humana y ha dado lugar a nuevos actores. En palabras de Gerunov, los fenómenos digitales son impredecibles y no están limitados físicamente[6].

El aumento de información disponible ha hecho de las fuentes abiertas (OSINT) y las redes sociales (SOCMINT) fuentes valiosas de inteligencia, así como imprescindible el empleo de nuevas herramientas tecnológicas para su tratamiento y discriminación, especialmente en lo relativo a las interacciones entre los actores y sus relaciones (teoría de redes), la desinformación y la politización de contenidos.

Sin embargo, estas nuevas herramientas también plantean nuevos desafíos éticos y prácticos a los procesos de inteligencia, a los que somete a un cambio metodológico significativo[7], al mismo tiempo que sobrecargan el trabajo de los analistas durante la obtención y la elaboración. La obtención ya no sólo se enfrenta a la velocidad de difusión de la información y al aumento de su volumen, sino también a dilemas éticos, dada la difusa zona gris entre lo privado y lo público de lo que se publica y es accesible. Su obtención puede ser legal, pero quizás no su explotación, especialmente en el marco de la inteligencia corporativa o empresarial.

Este cambio es tan profundo que el modelo de producción de inteligencia ha mutado por completo, tal como se detalla en la siguiente tabla comparativa que ilustra el contraste entre el paradigma tradicional (al que denominaremos como 1.0) y el evolucionado, digital o emergente (4.0), según como prefiramos llamarle. El paradigma tradicional de inteligencia, a pesar de operar en la «industria de la información», ha visto pocos cambios en sus procesos desde el inicio de la revolución digital[8]. Esta inercia es un riesgo existencial,

4. «Concepto que describe una situación de incertidumbre elevada, donde los hechos son inciertos, los valores están en conflicto, los riesgos son altos y las decisiones son urgentes, lo que vuelve ineficaces los métodos tradicionales de análisis», según Functowicz y Ravetz; Serra del Pino, J., «Anticipando en tiempos postnormales», en Arteaga, F., Ríos Insúa, D. (coords.): *El analista de inteligencia en la era digital*, Real Instituto Elcano, Centro Nacional de Inteligencia, 2022, pág. 55.

5. Pherson, R. H., Arcos, R., *Intelligence communication, op. cit.,* pág. 57.

6. Gerunov, A., *Risk analysis for the digital age*, Springer, 2023.

7. Véase Stenslie, S., Haugom, L., Vaage, B. H., *Intelligence analysis in the digital age*, Routledge, Abingdon, 2021, cap. 5.

8. Pherson, R. H., Arcos, R., *Intelligence communication, op. cit.,* pág. 2.

ya que la incapacidad de modernizar las operaciones podría conducir a una inminente obsolescencia de las organizaciones de inteligencia. La misión, tal como planteaban Pherson y Arcos hace más de una década, es transformar el análisis de inteligencia de un producto estático y narrativo a un formato más dinámico, digital e interactivo[9]. Esto obliga a los analistas a repensar los fundamentos de la comunicación y a reconocer que su capacidad para transmitir juicios de forma clara, concisa y creativa es lo que proporcionará una ventaja competitiva a sus organizaciones.

| Aspecto de la Inteligencia | Paradigma Tradicional (1.0) | Paradigma Digital (4.0) |
|---|---|---|
| Enfoque de Producción | «Push» (informes que se envían al cliente) | «Pull» (el cliente busca y accede al conocimiento) |
| Valor Principal | Acumulación de secretos (foco en la colección) | Creación de conocimiento y análisis (foco en el análisis) |
| Tecnología Clave | Archivos físicos, bases de datos aisladas | IA, Big Data, computación cuántica, redes sociales |
| Producto Final | Documento estático, informes escritos, papel | Producto multimedia interactivo y dinámico |
| Rol del Analista | Guardián del conocimiento, escritor | Asesor, narrador, comunicador estratégico |

*Tabla 1. Comparación de los Paradigmas 1.0 y 4.0 Fuente: elaboración propia*

Si a las herramientas tecnológicas sumamos las capacidades de la IA para analizar grandes volúmenes de datos, vínculos causales complejos, seguir indicadores y proporcionar alertas tempranas, estamos sumando al razonamiento lógico de los analistas y a su inteligencia social y emocional, una mayor capacidad autónoma de realizar tareas específicas de análisis, en menor tiempo, así como el abordar problemas complejos mediante la combinación de múltiples capas de procesamiento. Eso sí, sin obviar identificar en qué tareas son especialmente buenos los algoritmos y en cuales la creatividad y el razonamiento humano, o la combinación de ambos. Surge así el concepto de análisis de inteligencia aumentada, para referirse al uso de la IA para mejorar la inteligencia humana en lugar de operar de manera independiente o reemplazarla por completo[10].

El presente trabajo analiza las características, competencias y desafíos del Analista de Inteligencia 4.0 proponiendo un marco conceptual y operativo que permita su desarrollo profesional en organizaciones públicas y pri-

9. *Ibid*., págs. 1-2.

10. Babuta, A., *Artificial Intelligence and UK National Security*, Rusi, 2020, pág. 11.

vada. Para ello, se parte de la comparación anterior en el paradigma tradicional (1.0 y el emergente o digital (4.0), como base para entender la magnitud del cambio.

## 2. El ecosistema de la información en la era digital: desafíos y oportunidades

La digitalización ha desencadenado una explosión masiva de datos y ha multiplicado la conectividad global, un proceso que, si bien ofrece inmensas oportunidades, también erosiona la seguridad al facilitar la propagación acelerada de riesgos[11]. El desafío principal para las organizaciones de inteligencia ya no es la escasez de información, sino la abrumadora sobrecarga de datos (*Big Data*) y la incapacidad de analizarlos de manera efectiva con metodologías convencionales[12]. La paradoja de la sobreabundancia de datos es evidente: a pesar de tener acceso a una cantidad sin precedentes de información, la capacidad para generar inteligencia procesable y oportuna no ha crecido al mismo ritmo[13]. El problema fundamental ha pasado de ser la «escasez de datos» a la «escasez de significado». Este cambio se ve exacerbado por el incesante flujo de noticias 24/7 en nuestros dispositivos móviles, que impone nuevos patrones de comportamiento en los tomadores de decisiones y, por consiguiente, en los productores de inteligencia.

En este nuevo ecosistema, los servicios de inteligencia ya no ostentan el monopolio de la información[14]. Deben competir de manera directa con fuentes de inteligencia privadas que, en muchos casos, disponen de mayores recursos y menos restricciones operativas para generar inteligencia estratégica. Esta situación ha reducido la ventaja comparativa tradicional de los servicios públicos frente a sus usuarios, tanto en el ámbito gubernamental como en el privado, y ha forzado una redefinición de su propuesta de valor. La proliferación de la inteligencia «como servicio»[15] obliga a los servicios públicos a innovar y a buscar la colaboración con otros actores. Este panorama competitivo, si bien es un desafío, se presenta también como una oportunidad para la integración de comunidades de inteligencia de distinto perfil (públicas y privadas) y para el desarrollo conjunto de nuevos métodos y estrategias[16].

---

11. Arteaga, F., Fonfría, A., «La inteligencia en el siglo XXI», en Arteaga, F., Ríos Insúa, D. (coords.): *El analista de inteligencia en la era digital*, Real Instituto Elcano, Centro Nacional de Inteligencia, 2022, pág. 12.
12. Gerunov, A., *Risk analysis..., op. cit.,* pág. 81.
13. Stenslie, S., Haugom, L., Vaage, B. H., *Intelligence analysis, op. cit.,* pág. 52.
14. Arteaga, F., Fonfría, A., «La inteligencia...», *op. cit*., pág 14 y 15.
15. Arteaga, F., Fonfría, A., «La inteligencia...», *op. cit*., pág. 14.
16. *Ibid*., págs. 18 y 19.

El impacto de la digitalización se extiende a la proliferación de la desinformación y las operaciones de influencia, que se propagan a una velocidad viral en las redes de comunicación social[17]. Tecnologías emergentes como los *deepfakes* complican aún más el panorama, obligando a una nueva vigilancia. El Analista 4.0 no solo debe analizar a los potenciales agresores, sino también monitorizar y comprender estas «fuentes de fractura y radicalización interna» para poder advertir a tiempo a los decisores sobre sus consecuencias[18]. En este contexto, el analista debe lidiar con la complejidad, la velocidad y un «alto riesgo» que exigen una reevaluación de la metodología de evaluación y, de manera crucial, de la transmisión del mensaje[19]. Los cambios de paradigma no son solo cuestión de eficiencia, sino una necesidad imperativa para la viabilidad y supervivencia de la comunidad de inteligencia en un mundo donde la información es abundante y los clientes demandan un acceso instantáneo y personalizado a los análisis[20].

Además, la transformación digital ha modificado los patrones de consumo de inteligencia. Las generaciones Y, Z y Alpha, nativas digitales, demandan productos analíticos accesibles, interactivos y personalizados, adaptados a sus hábitos de lectura, dispositivos móviles y expectativas cognitiva. Esta demanda crece imparable. Las generaciones Y y Z (*zoomers* o *centennials*), la de los verdaderos nativos digitales, superan los 30 años y comienzan a escalar como decisores, alcanzando puestos de dirección.

| **Generaciones sociales de Occidente<br>*Rango de años aproximado** | |
|---|---|
| Generación perdida | Mayores de edad durante la IGM. |
| Generación grandiosa | Nacidos entre 1901 y 1927 |
| Generación silenciosa | Nacidos entre 1928 y 1945 |
| *Baby boomer,* jubilados en su mayor parte. | Personas nacidas entre 1946 y 1964 |
| Generación X. El mundo comienza a transformarse con la llegada de las nuevas tecnologías. | Personas nacidas entre 1965 y 1981 |
| Generación Y (*milennials*). Las tecnologías han estado presentes en la mayor parte de sus vidas = nativos digitales. | Entre 1991 y 1996 |
| Generación Z (*zoomers* o *centennials*) han utilizado Internet desde muy joven y se sienten cómodos con la tecnología y los medios sociales = verdaderos nativos digitales | Personas nacidas a mediados de la década de 1990 y finales de la década de los 2000 |

17. *Ibid*., pág. 12.
18. *Idem.*
19. Pherson, R. H., Arcos, R., *Intelligence communication, op. cit.*, pág. 2.
20. *Idem.*

| Generaciones sociales de Occidente<br>*Rango de años aproximado | |
|---|---|
| Generación Alpha, completamente nativa digital con exposición temprana a dispositivos inteligentes y la IA | Personas nacidas a principios de la década de 2010 y mediados de la década de 2020. |
| Generación Beta, de inmersión total en la IA, la automatización y la hiperconectividad desde su nacimiento | Nacidos a partir de mediados de la década de 2020 |

*Tabla 2. Relación de las generaciones occidentales con la TIC Fuente: elaboración propia*

Esta evolución, más que cambio, implica nuevos retos y oportunidades para los analistas, como todo lo que muta con el tiempo.

## 3. La adopción de tecnologías emergentes: big data, IA y computación

La Inteligencia Artificial se ha convertido en una ventaja estratégica fundamental para la comunidad de inteligencia, ya que permite maximizar la efectividad y eficiencia en la obtención, el procesamiento y la explotación de grandes volúmenes de datos[21]. La IA se aplica en áreas críticas como la identificación de objetivos, el análisis de datos masivos y la detección de amenazas internas[22]. Sin embargo, la adopción de estas tecnologías implica una redefinición del juicio humano, no su obsolescencia.

La imperativa de la colaboración humano-máquina se basa en la premisa de que la IA no reemplaza al analista, sino que lo «empodera»[23]. El rol del analista humano se vuelve aún más vital, ya que es el responsable de alimentar los programas con datos de calidad, de formular las preguntas estratégicas correctas y de reconocer cuándo la realidad o el entorno han cambiado lo suficiente como para requerir nuevos modelos o enfoques[24]. La IA asume la carga cognitiva de procesar lo masivo y lo repetitivo, liberando al analista para concentrarse en el pensamiento estratégico, la formulación de hipótesis complejas y la resolución de problemas impredecibles.

21. Babuta, A., *Artificial Intelligence..., op. cit.,* pág. 13.

22. Véase Lucchini, L., *CYBERUK 2023 blog. Perspectives on change: AI ethics in the intelligence lifecycle*, Deloitte United Kingdom, 2023.

23. Gillespie, N., Rowlands, D., *The age of Intelligence..., op. cit.,* pág. 79.

24. Carnicero González, I. J. «Tendencias en la modelización de riesgos de entidades financieras», en Arteaga, F., Ríos Insúa, D. (coords.): *El analista de inteligencia en la era digital*, Real Instituto Elcano, Centro Nacional de Inteligencia, 2022, pág. 112.

Esta liberación de capacidad analítica se opera mediante la adopción de un ecosistema de herramientas digitales avanzadas. Plataformas de análisis de redes y enlaces como *Maltego* o *i2 Analyst's Notebook* permiten mapear y visualizar relaciones complejas entre entidades (personas, organizaciones, transacciones) a partir de grandes volúmenes de datos heterogéneos. Para el análisis de fuentes abiertas (OSINT), las herramientas de Procesamiento del Lenguaje Natural (NLP), como *MonkeyLearn* o las *APIs* de *OpenAI*, automatizan tareas de análisis de sentimiento, clasificación temática y extracción de entidades en tiempo casi real. Asimismo, el dominio de lenguajes de programación como Python y sus librerías de *Machine Learning* (por ejemplo, *Scikit-learn* o *TensorFlow*) se ha vuelto crucial para desarrollar modelos propios de detección de anomalías, clasificación de amenazas o predicción de tendencias, sentando la base para el siguiente escalón analítico: la modelización y simulación.

Más allá del análisis de datos masivos, el Analista 4.0 debe utilizar la modelización y la simulación como herramientas esenciales[25]. Un oficio analítico centrado en modelos ofrece nuevas oportunidades para abordar los problemas de la relación entre productores y consumidores de inteligencia al capitalizar los recursos computacionales[26]. Estas capacidades permiten a los analistas explorar múltiples futuros posibles, entender las compensaciones (*tradeoffs*) entre diferentes conjuntos de datos y modelos, y evaluar la eficacia de las posibles acciones políticas[27], o de cualquier tipo. Este enfoque representa un cambio significativo de la «predicción» a la «exploración de escenarios», lo que reduce la incertidumbre en la toma de decisiones al proporcionar un mapa de posibles resultados y sus respectivas dependencias de variables y suposiciones[28]. Los modelos basados en agentes (*Agent-Based Modeling* o ABM) se presentan como una herramienta particularmente superior para el análisis estimativo. En lugar de buscar un resultado único, los ABM permiten a analistas y clientes examinar múltiples escenarios contrafactuales, entendiendo el espacio de compensación entre diferentes conjuntos de datos, modelos conceptuales y opciones de política[29].

Sin embargo, la adopción acelerada de la IA introduce riesgos que requieren una gestión reflexiva y proactiva. Un estudio de KPMG revela que un 66 % de las personas confían en la salida de la IA sin evaluar su precisión, y un 56 % admite haber cometido errores en su trabajo debido a esta confianza[30]. Esta

25. Pherson, R. H., Arcos, R. *Intelligence communication, op. cit.*, pág. 89.

26. Aaron, F., «Transforming Producer/Consumer Relations through Modeling and Computation», en Pherson, R. H., Arcos, R. (eds.): *Intelligence communication in the digital era: Transforming security, defence and business*, Palgrave Macmillan, Basingstoke, 2015, pág. 91.

27. *Ibid*., pág. 101.

28. *Idem*., pág. 101.

29. *Ibid.*, pág. 97-98.

30. Gillespie, N., Rowlands, D., *The age of Intelligence..., op. cit,* pág. 75.

estadística es preocupante, ya que una confianza ciega en las máquinas puede llevar a errores críticos en la producción de inteligencia. Esta situación subraya la importancia de la «alfabetización en IA» (*AI literacy*) como una competencia esencial[31] para mitigar este riesgo. Este fenómeno genera una cadena de causalidad crítica: la adopción de la IA incrementa la dependencia de sus resultados, lo que a su vez aumenta el riesgo de errores por falta de verificación humana. Para mitigar esto, es crucial fomentar la «confianza» en la IA a través de la transparencia y la *explicabilidad*[32] (sobre cómo se toman las decisiones) y de fortalecer la «alfabetización en IA» en los equipos.

A nivel geopolítico, especialmente a partir de la pandemia de COVID-19 y la crisis de la cadena de suministro, la IA también se está convirtiendo en una cuestión de soberanía nacional y poder geopolítico. El concepto de «IA Soberana»[33] demuestra que las naciones están compitiendo por controlar los datos y la infraestructura tecnológica dentro de sus propias fronteras para garantizar la seguridad nacional y el cumplimiento de regulaciones y su crecimiento económico. Esto añade una nueva capa de análisis al entorno, ya que la dependencia tecnológica de proveedores extranjeros se convierte en una vulnerabilidad estratégica[34], tanto en los niveles nacionales como corporativos.

## 4. La gestión del riesgo y la incertidumbre en la toma de decisiones

El universo del riesgo se ha expandido de manera dramática y es más complejo de comprender y analizar con herramientas tradicionales[35]. La digitalización ha facilitado la propagación de riesgos de diversa índole (económicos, medioambientales, geopolíticos y tecnológicos) a una velocidad sin precedentes[36]. En este entorno, la comunicación del riesgo se vuelve un arte que va más allá de los datos y las estadísticas. Para que la

31. *Ibid*., 77.

32. Véase Lucchini, L., *CYBERUK 2023 blog, op. cit.*

33. Alduhishy, M., *Sovereign AI: What it is, and 6 strategic pillars for achieving it*, World Economic Forum, 2024. Disponible en: https://www.weforum.org/stories/2024/04/sovereign-ai-what-is-ways-states-building/

34. *The Future of Intelligence Analysis. A task-level view of the impact of artificial intelligence on intel analysis*, Deloitte, 2019.
Disponible en: https://www.deloitte.com/us/en/insights/industry/government-public-sector-services/artificial-intelligence-impact-on-future-intelligence-analysis.html

35. Véase Gerunov, A., *Risk analysis..., op. cit.*

36. Artigas, C., «El potencial de la Inteligencia Artificial en el ámbito de la inteligencia estratégica y la seguridad», en Arteaga, F., Ríos Insúa, D. (coords.): *El analista de inteligencia en la era digital*, Real Instituto Elcano, Centro Nacional de Inteligencia, 2022, pág. 125

información sea asimilada por los decisores, debe infundirse de «afecto» (emoción), es decir, de un componente emocional que la haga más tangible y memorable[37].

La comunicación eficaz del riesgo implica un enfoque que combine la lógica (pensamiento analítico) con la emoción (pensamiento experiencial)[38]. Un informe que se limita a cifras abstractas puede ser menos efectivo que una narrativa que contextualice el riesgo y lo haga tangible a través de elementos visuales, como gráficos, infografías o animaciones. Un analista puede, por ejemplo, ilustrar la escala de una amenaza comparándola con un fenómeno conocido por el decisor, lo que le permite conectar el dato abstracto a una experiencia concreta para un mejor entendimiento[39]. La importancia de esto se refleja en la supuesta cita de Stalin: «La muerte de un hombre es una tragedia; la muerte de millones es una estadística»[40]. Para superar este desafío, los analistas deben aprender a «infundir las estadísticas con afecto» para hacer que el riesgo sea más «tangible y memorable», por ejemplo, pasando de porcentajes abstractos a frecuencias concretas (por ejemplo, «10 de cada 100» en lugar de «10 %») o «humanizando» las historias para evocar una respuesta empática que complemente el análisis racional[41].

En un entorno de «profunda incertidumbre»[42] el analista ya no busca una única respuesta, sino que proporciona un mapa de compensaciones (*tradeoffs*) y escenarios posibles[43]. La aplicación de técnicas estructuradas de análisis (SAT) y la modelización se convierten en la clave para gestionar esta incertidumbre y proporcionar un análisis transparente y robusto. El desafío ético reside en equilibrar la objetividad, que es la base de la inteligencia, con el componente persuasivo y emocional requerido para la comunicación de impacto. La meta no es manipular al decisor, sino asegurar que la información crítica no sea ignorada debido a su formato o presentación.

Este panorama genera una clara cadena de causalidad en la que un entorno de elevada incertidumbre aumenta la complejidad de los riesgos a considerar. Esto, a su vez, hace que los métodos tradicionales de comunicación de riesgo sean ineficientes, especialmente ante una audiencia más hiperconectada y acostumbrada a recibir información por diferentes canales y formas diversas, creando la necesidad de comunicar el riesgo de manera

37. Pyrik, J., «Communicating Risk», en Pherson, R. H., Arcos, R. (eds.): *Intelligence communication in the digital era: Transforming security, defence and business*, Palgrave Macmillan, Basingstoke, 2015, pág. 44.

38. *Ibid.,* pág. 45-46.

39. *Ibid*., pág. 49.

40. *Ibid*., pág. 47.

41. *Ibid*., pág. 49.

42. Aaron, F., «Transforming Producer..., *op. cit.,* pág. 91.

43. Aaron, F., «Transforming Producer..., *op. cit*., págs. 101-102.

más persuasiva a través del «afecto» (emoción) y la contextualización. Por lo tanto, un Analista de Inteligencia 4.0 no solo debe identificar los riesgos, sino también entender cómo el decisor los percibe y adaptar la comunicación para que sea asimilable y conduzca a la acción. Los factores de percepción de riesgo más importantes, como la Confianza, el Beneficio, la Elección y el Control, deben ser tomados en cuenta por el analista experto para personalizar su mensaje[44].

## 5. La nueva filosofía de producción analítica

La filosofía de producción de inteligencia ha experimentado un cambio radical descrito en la introducción: la transición del modelo tradicional de *«push»* al modelo digital de *«pull»*. El usuario puede buscar, acceder y personalizar la información según su interés y en el momento que lo necesite, o lo recibe en una acción de *«push»* (la remisión habitual durante la fase de difusión del producto de inteligencia) a la que está suscrito, o no. Este nuevo paradigma requiere un cambio fundamental en el diseño de los productos analíticos, que deben ser más dinámicos, modulares y fáciles de navegar. En definitiva, más «atractivos» para los usuarios de inteligencia, porque su experiencia digital es cada vez más individual y personalizada.

Para ilustrar este modelo, imagine un *dashboard* (cuadro de mando) de inteligencia geopolítica, alojado en una plataforma como *Sharepoint*, *Tableau* o *Power BI*, donde el decisor puede filtrar interactivamente por país, tipo de riesgo (político, económico, social) y horizonte temporal. Este *dashboard* no solo mostraría datos históricos, sino también pronósticos (*forecasts*) generados por IA, y permitiría la descarga de briefings personalizados en PDF adaptados a los criterios de selección del usuario. La colaboración se ha convertido en el eje central de la producción de inteligencia en la era digital. El trabajo en silos, donde cada agencia o departamento produce su propia versión de un mismo tema, está siendo reemplazado por la «inteligencia colectiva»[45]. Plataformas colaborativas, como los wikis (por ejemplo, *Intellipedia*, BICES en OTAN o un simple *Sharepoint* en el entorno corporativo), permiten a analistas de distintas agencias, departamentos y disciplinas trabajar en un mismo documento, evitando la duplicidad de esfuerzos y generando consenso de manera temprana en el proceso[46]. Este enfoque acelera la producción y mejora la calidad del análisis al integrar

44. Pyrik, J., «Communicating...», *op. cit.,* págs. 50-53.

45. Véase Arteaga, F., Ríos Insúa, D. (coords.): *El analista de inteligencia en la era digital*, Real Instituto Elcano, Centro Nacional de Inteligencia, 2022.

46. Pherson, R. H., «Establishing a New Paradigm of Collaboration», en Pherson, R. H., Arcos, R. (eds.): *Intelligence communication in the digital era: Transforming security, defence and business*, Palgrave Macmillan, Basingstoke, 2015, pág. 59.

múltiples perspectivas y fuentes de experiencia. Los entornos de colaboración basados en avatares[47], facilitan aún más la interacción sincrónica y la comunicación entre analistas y decisores, eliminando las barreras geográficas y los desafíos de programación[48]. El análisis basado en wikis difumina los límites entre los roles de obtención, análisis y decisión, permitiendo aprovechar la experiencia de cada persona y sus contribuciones, sin importar su afiliación organizativa[49]. Se ha pasado de un proceso lineal en serie a uno más colaborativo en el que los analistas deben dominar las herramientas digitales que lo facilitan y posibilitan en mayor medida.

En este mundo tan sobrecargado de información que estamos describiendo, el analista 4.0 debe dominar lo que se ha denominado *«presentational tradecraft»* para «capturar la atención del cliente»[50]. Esto implica ir más allá del texto y utilizar infografías, videos, mapas interactivos y visualizaciones de datos para contar una historia de manera clara, concisa y convincente. La presentación debe ser diseñada para ser memorable y procesable. Dado que los gráficos permiten simplificar datos, comparar fácilmente variables, entender la información de forma intuitiva y captar la atención de los decisores, su empleo es de gran importancia en este nuevo entorno de producción de inteligencia. No menos importante es la comunicación auditiva o interactiva. Eso sí, adaptada también a los dispositivos digitales móviles, que individualizan la experiencia de los usuarios. Para comunicar con éxito, el analista debe aplicar principios de diseño como la proximidad, alineación, contraste y repetición, además de los principios de persuasión para que las ideas «se adhieran» a la mente del consumidor[51], a los que ha de llegar de forma atractiva. Es precisamente la saturación informativa la que ha hecho que la fase de difusión de inteligencia haya cobrado más importancia que nunca.

## 6. Ética y gobernanza de la inteligencia digital

El análisis actual exige multidisciplinariedad, trabajo en equipo y herramientas colaborativas avanzadas para compartir modelos y visualizaciones de grandes volúmenes de datos. La ventaja competitiva radica en la «ventaja analítica». La inteligencia ha evolucionado, centrando el proceso en el análisis y requiriendo que los analistas asuman nuevos roles con herramientas avanzadas como, por ejemplo, la inteligencia artificial. Sin embargo, los analistas

47 Un avatar es la representación digital del usuario dentro de un entorno virtual.

48. Pherson, R. H., «Establishing a New Paradigm…», *op. cit.*, pág. 69.

49. *Ibid.*, pág. 60.

50. O´Sullivan, M. «Presentational Tradecraft: A New Skill», en Pherson, R. H., Arcos, R. (eds.): *Intelligence communication in the digital era: Transforming security, defence and business*, Palgrave Macmillan, Basingstoke, 2015, pág. 24.

51. *Ibid.*, pág. 36-39.

y sus organizaciones deben adoptar estos avances de manera equilibrada, con estrategias claras de uso, formación y reconfiguración de procesos, alineadas con la ética empresarial. Esto permitirá a los analistas enfocarse en tareas creativas y estratégicas, mejorando la anticipación y reacción ante amenazas, pero manteniendo las herramientas avanzadas, como la IA, bajo la supervisión y el control humano, esencial para mitigar riesgos de seguridad. privacidad y ética, bajo estrictos modelos de gobernanza,

La adopción de la IA en inteligencia introduce un imperativo ético de gran importancia. La «algoritmización» de las decisiones conlleva riesgos nuevos, como el «sesgo algorítmico» (*algorithmic bias*), que puede sesgar las predicciones de forma no intencionada, socavando así la imparcialidad del análisis[52]. Esto plantea serias preguntas sobre la adhesión a los principios fundamentales de las democracias liberales occidentales. Por ejemplo, los sistemas de detección pueden generar perfiles de riesgo basados en datos con sesgos históricos, lo que perpetúa la discriminación en la toma de decisiones.

La mitigación proactiva de este riesgo exige ir más allá de los principios y implementar procesos técnicos concretos, como las auditorías algorítmicas (*algorithmic auditing*), tal y como recomiendan marcos de gobernanza internacionales como el de la OCDE[53]. Estas auditorías consisten en la evaluación sistemática y regular de los conjuntos de datos de entrenamiento, los modelos y sus resultados, con el fin de identificar, cuantificar y corregir sesgos no intencionados, garantizando así la equidad y la ausencia de discriminación en las decisiones apoyadas por la IA.

Un desafío operativo intrínseco a muchos modelos avanzados, como los de *deep learning*, es su naturaleza de «caja negra» (*black-box*), donde las razones detrás de una decisión o predicción son opacas incluso para sus desarrolladores. Esta falta de transparencia es un obstáculo crítico para la auditoría, la confianza y la rendición de cuentas. Para superarlo, es imperativo el desarrollo e implementación de técnicas de IA Explicable (*Explainable AI* o *XAI*), un campo dedicado a crear métodos e interfaces que permitan a los analistas humanos comprender, confiar y gestionar efectivamente las recomendaciones generadas por la IA. El NIST, de hecho, establece que para que un sistema de IA sea explicable debe proporcionar evidencias, razones y una comprensión clara de su funcionamiento[54].

Para mitigar estos riesgos, el modelo de gobernanza de Deloitte[55] propone un marco de tres pilares para una IA responsable en el ciclo de inteligencia:

52. Véase Lucchini, L., *CYBERUK 2023 blog..., op. cit.*

53. OCDE, *Recommendation of the Council on Artificial Intelligence*, 2019.

54. Véase Rudin, C., *Four Principles of Explainable Artificial Intelligence*, National Institute of Standards and Technology (NIST), 2020.

55. Véase Lucchini, L., *CYBERUK 2023 blog..., op. cit.*

Identificación de sus propósitos e impactos conforme a los objetivos y valores de la organización, lo que exige definir el objetivo de la IA y calibrar las consecuencias, intencionadas o no, sobre los individuos afectados.

Adopción de un enfoque justo y equitativo, que asegura que la tecnología y los datos obtenidos y almacenados cumplan con las regulaciones de seguridad, derechos humanos, protección de datos personales y leyes antidiscriminación.

Mantenimiento de valores centrados en el ser humano, de tal forma que se garantice la transparencia de los sistemas empleados, y su *explicabilidad*, en cuanto a su capacidad de ser comprendidos, para que tanto los analistas como la sociedad puedan confiar en ellos y entenderlos.

El modelo de Deloitte se alinea y es complementado por otros marcos de gobernanza de la IA de alcance global. Las directrices para una IA confiable de la Unión Europea[56], basadas en los principios de respeto de la autonomía humana, prevención del daño, equidad y *explicabilidad*, y las Principios de IA de la OCDE[57], que incluyen el crecimiento inclusivo y el bien social, constituyen esfuerzos fundamentales para establecer principios rectores para el desarrollo y despliegue ético de estas tecnologías a escala internacional. La convergencia hacia estos estándares es crucial para la interoperabilidad y la legitimidad de los sistemas de IA utilizados en inteligencia.

La confianza no es solo una cuestión de seguridad técnica, sino un componente esencial para la viabilidad de la inteligencia en la era digital. Un estudio de KPMG revela una tensión crítica: a pesar de la adopción masiva de la IA (66 % de las personas la usan regularmente), solo el 46 % de ellas confía en estos sistemas[58]. Esta desconfianza pública, junto con el riesgo de errores no verificados (como el 66 % de personas que confían en los resultados de la IA sin evaluarlos), crea un «déficit de confianza» que los líderes deben abordar de manera proactiva a través de una gobernanza sólida y programas de educación[59]. Parece más que evidente que los riesgos que genera el empleo de la IA u otras herramientas avanzadas futuras (procesamiento cuántico), especialmente los de índole ética, no deben gestionarse de forma aislada, sino como un entramado que integra la gobernanza, el riesgo y el cumplimiento.

A continuación, se presenta una matriz que relaciona los principales riesgos éticos de la IA con las acciones de mitigación propuestas.

---

56. Grupo de Expertos de Alto Nivel en IA de la Comisión Europea, *Directrices éticas para una IA confiable*, 2019. Disponible en: https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai

57. OCDE, *Recommendation of the Council on Artificial Intelligence*, 2024.

58. Gillespie, N., Rowlands, D., *The age of Intelligence..., op. cit.,* pág. 5.

59. *Ibid.,* pág. 97.

| Riesgo Ético | Ejemplo o Consecuencia | Acciones de Mitigación |
|---|---|---|
| Sesgo Algorítmico | Las predicciones se sesgan de forma no intencionada, socavando la imparcialidad y la adhesión a principios democráticos | Auditorías de algoritmos (uso del marco de 3 pilares de Deloitte o similar) |
| Falta de Confianza | La desconfianza pública y de los analistas en los sistemas de IA dificulta su adopción y la validez de sus resultados | Fortalecimiento de la gobernanza y la alfabetización en IA, programas de educación sobre la tecnología |
| Pérdida de Control | Los decisores pierden el control sobre la toma de decisiones al delegar en sistemas de IA cuyos procesos no comprenden | Mantenimiento de valores centrados en el humano, asegurando la transparencia y *explicabilidad* de los modelos |

*Tabla 3. Riesgos Éticos de la IA y sus medidas de mitigación*

## 7. El perfil y las competencias del analista 4.0

El perfil del Analista de Inteligencia 4.0 se basa en la multidisciplinariedad, multifuncionalidad y la resiliencia. Debe combinar la experiencia y la especialización en diversidad de áreas (geopolítica, economía, seguridad, defensa, derecho, matemáticas, ciencia de datos, etc.) con la capacidad de adaptarse a los entornos complejos e inciertos[60] descritos en la introducción (VUCA, BANI, post-normales). La resiliencia y la capacidad de perseverar son cruciales en estos entornos de incertidumbre y ambigüedad, donde los desafíos son constantes y las soluciones no son siempre claras, pero sí urgentes. La autogestión del aprendizaje continuo y el escepticismo

60. Páramo, A., «El analista de inteligencia...», *op. cit.*, pág. 21.

metodológico se vuelven factores clave para reforzar la credibilidad del analista. Esto implica una revisión constante de sus herramientas de trabajo, sus supuestos y sus marcos de análisis para adaptarse a una realidad en perpetuo cambio[61]. Por ejemplo, un analista que, tras un evento de cisne negro (como una pandemia o un conflicto inesperado), no solo actualiza sus datos, sino que revisa críticamente los modelos predictivos que fallaron y busca incorporar nuevas variables o técnicas, demostrando así una capacidad de adaptación que sustenta su credibilidad y valor.

El papel del pensamiento crítico es más importante que nunca. En un mundo sobrecargado de datos, el analista debe ser capaz de «pensar en los extremos»[62], evitar sesgos cognitivos y reconocer cuándo la realidad ha cambiado y los modelos de análisis deben ser actualizados[63]. Esta habilidad humana para formular las preguntas correctas y discernir la veracidad de la información es un complemento insustituible para los sistemas automatizados. La capacidad de pensamiento crítico, junto con la alfabetización en IA, son fundamentales para evitar la dependencia ciega de la tecnología[64].

En este nuevo paradigma, el analista no solo produce un informe, sino que se convierte en un asesor de confianza para el decisor, ayudándolo a pasar de la «inteligencia» a la «acción»[65]. El documento de KPMG[66] resalta el papel del analista en «desbloquear valor, innovación y estrategia» para su organización, lo que refuerza la idea de que su rol es el de un catalizador de la acción, más que el de un simple configurador de modelos o proveedor de datos.

Por último, los analistas y sus líderes deben de ser pacientes. Conjuntar un equipo nunca ha sido fácil, como tampoco lo ha sido el adquirir conocimiento diverso. Tampoco lo es ahora, ya se han tratado los motivos, pero el fundamental es que requiere tiempo y asumir fracasos.

La siguiente tabla resume las competencias esenciales del Analista de Inteligencia 4.0, integrando los conocimientos discutidos a lo largo del presente trabajo.

---

61. Stenslie, S., Haugom, L., Vaage, B. H., *Intelligence analysis in the digital age*, Routledge, Abingdon, 2021, pág. 168.

62. Pherson, R. H., Arcos, R., *Intelligence communication, op. cit.*, pág. 9.

63. Stenslie, S., Haugom, L., Vaage, B. H., *Intelligence analysis..., op. cit.*, pág. 2.

64. Gillespie, N., Rowlands, D., *The age of Intelligence..., op. cit.,* pág. 84.

65. Calof, J., «Creating Impactful Intelligence: Communication Lessons from the Corporate Environment», en Pherson, R. H., Arcos, R. (eds.): *Intelligence communication in the digital era: Transforming security, defence and business*, Palgrave Macmillan, Basingstoke, 2015, pág. 73.

66. Gillespie, N., Rowlands, D., *The age of Intelligence..., op. cit.*, pág. 96.

| Categoría | Competencias Clave | Descripción y Contexto | Herramientas / Manifestaciones prácticas |
|---|---|---|---|
| Habilidades | Pensamiento Crítico | Capacidad para analizar información compleja, identificar sesgos y formular preguntas estratégicas. La diversidad es clave. | Uso de técnicas estructuradas de análisis (ACH - *Analysis of Competing Hypotheses*, *Devil's Advocacy*); empleo de herramientas de diagramas (*Miro, Lucidchart*) para mapear lógica y suposiciones. |
| | Alfabetización en IA y herramientas avanzadas | Comprensión de cómo funcionan los sistemas y capacidad para evaluar la precisión de sus resultados. | Interacción con LLMs (ChatGPT, Claude) para generación de hipótesis; depuración de código en Python; interpretación de resultados de modelos de *clustering* o clasificación (*Scikit-learn*); uso de herramientas de auditoría de sesgos (IBM AI *Fairness* 360). |
| | Comunicación de Impacto | Habilidad para usar narrativas y visualizaciones (infografías, mapas) para hacer la inteligencia más tangible, atractiva y asimilable para el decisor. | Dominio de software de visualización (*Tableau, Power BI, Flourish*); diseño básico (*Canva, Adobe Express*); creación de *dashboards* interactivos; *storytelling* con datos. |

| Categoría | Competencias Clave | Descripción y Contexto | Herramientas / Manifestaciones prácticas |
|---|---|---|---|
| Conocimientos | Big Data y Análisis | Capacidad para obtener, organizar, modelar y crear valor a partir de un universo de datos masivos y heterogéneos. | Uso de entornos de programación (*Jupyter Notebooks*); manejo de librerías de datos (*Pandas, NumPy);* consulta de bases de datos (SQL, NoSQL); procesamiento de datos a gran escala (*Spark*). |
| | Multidisciplinar (con amplia base en geopolítica, teoría de redes e idiomas) | Comprensión de la complejidad del entorno global y cómo los riesgos se propagan a través de la conectividad. | Uso de herramientas de análisis de redes (*Gephi, Maltego*) para mapear relaciones; aplicación de modelos de simulación (*agent-based modeling* con *NetLogo*); seguimiento de fuentes primarias en idiomas originales. |
| Valores | Integridad y Proactividad | Mantenimiento de la objetividad, frente a la presión interna, política y social, así como de la capacidad de anticiparse a los eventos. | Aplicación de marcos éticos (Directrices UE, OCDE, AEPD) en los informes; uso de herramientas de monitorización de tendencias (*Google Trends, Brandwatch; Bloomberg*) para identificación proactiva de amenazas y oportunidades; redacción de alertas tempranas. |
| | Resiliencia | Habilidad para perseverar y adaptarse a un entorno caracterizado por la incertidumbre, la complejidad y el cambio. | Empleo de metodologías ágiles (*Scrum, Kanban; MoSCow*) para gestión de proyectos; uso de plataformas de colaboración (*Slack, Teams*) para trabajo en equipo bajo presión; técnicas de gestión del estrés y priorización. |

*Tabla 4. Perfil del Analista 4.0: Habilidades, Conocimientos y Valores*

# 8. Conclusiones

El presente documento pretende demostrar que la digitalización, la IA y otras herramientas digitales avanzadas han catalizado una transformación profunda en el rol del analista de inteligencia, que seguirá progresando. El profesional del futuro inmediato, el Analista de Inteligencia 4.0, es un híbrido de estratega, comunicador y tecnólogo, cuyo valor radica en su capacidad para navegar un ecosistema sobrecargado de información, colaborar con sistemas inteligentes y gestionar el riesgo y la incertidumbre en beneficio de los decisores, de forma ágil y atractiva. La vieja dicotomía entre la obtención de secretos y la producción de análisis ha dado paso a un proceso centrado en el análisis, donde la creación de significado es la principal divisa. Para ello es cada vez más relevante el uso de herramientas analíticas avanzadas.

La profesión de la inteligencia se moverá inexorablemente hacia una mayor integración de capacidades de análisis apoyado en esas nuevas y más potentes herramientas analíticas, incluida la IA, y en la inteligencia colectiva y colaborativa. Los departamentos y servicios de inteligencia, empresariales o públicos, que adopten una cultura de innovación en IA o en cualesquiera otras herramientas avanzadas estarán mejor posicionados para preservar la continuidad y resiliencia de sus operaciones en el caso de los primeros, así como el estilo de vida y la seguridad nacional en el caso de los segundos, ya que podrán moverse más fácil y efectivamente del modo reactivo al proactivo, de mejores resultados ante la incertidumbre. En este sentido, el sector público tiene la oportunidad de aprender de la agilidad, los recursos y la orientación al cliente, al que puede perfilar mejor que nunca, que ha demostrado el sector privado para mantenerse relevante.

El futuro de la inteligencia no es ya una estructura monolítica, sino una comunidad de comunidades de inteligencia hiperconectada, donde los actores públicos y privados colaboran para buscar oportunidades y hacer frente a amenazas globales. El Analista 4.0 es la pieza clave para habilitar este ecosistema, ya que su perfil multifuncional le permite actuar como un puente entre la tecnología y el juicio humano, entre la sobreabundancia de datos y la escasez de significado, y, en última instancia, entre la inteligencia y la acción.

Por ello, la evolución hacia el Analista de Inteligencia 4.0 no es una opción, sino una imperativa de supervivencia estratégica. Las organizaciones que inviertan de forma decidida en este nuevo perfil, dotándolo no solo de tecnología avanzada, sino de la formación en alfabetización IA, los marcos éticos sólidos y la cultura de aprendizaje continuo que lo sustentan, serán las que construyan una ventaja analítica decisiva y lideren la toma de decisiones en la era de la incertidumbre digital.

# BIBLIOGRAFÍA

**Alduhishy, M.**, *Sovereign AI: What it is, and 6 strategic pillars for achieving it*, World Economic Forum, 2024.

**Artigas, C.**, «El potencial de la Inteligencia Artificial en el ámbito de la inteligencia estratégica y la seguridad», en Arteaga, F., Ríos Insúa, D. (coords.): *El analista de inteligencia en la era digital*, Real Instituto Elcano, Centro Nacional de Inteligencia, 2022.

**Arteaga, F.**, **Fonfría, A.**, «La inteligencia en el siglo XXI», en Arteaga, F., Ríos Insúa, D. (coords.): *El analista de inteligencia en la era digital*, Real Instituto Elcano, Centro Nacional de Inteligencia, 2022.

**Aaron, F.**, «Transforming Producer/Consumer Relations through Modeling and Computation», en Pherson, R. H., Arcos, R. (eds.): *Intelligence communication in the digital era: Transforming security, defence and business*, Palgrave Macmillan, Basingstoke, 2015.

**Babuta, A.**, *Artificial Intelligence and UK National Security*, Rusi, 2020.

**Calof, J.**, «Creating Impactful Intelligence: Communication Lessons from the Corporate Environment», en Pherson, R. H., Arcos, R. (eds.): *Intelligence communication in the digital era: Transforming security, defence and business*, Palgrave Macmillan, Basingstoke, 2015.

**Carnicero González, I. J.** «Tendencias en la modelización de riesgos de entidades financieras», en Arteaga, F., Ríos Insúa, D. (coords.): *El analista de inteligencia en la era digital*, Real Instituto Elcano, Centro Nacional de Inteligencia, 2022.

**Gerunov, A.**, *Risk analysis for the digital age*, Springer, 2023.

**Gillespie, N.**, **Rowlands, D.**, *The age of Intelligence. Empowering human-AI collaboration for a trusted future*, KPMG, 2025.

**Lucchini, L.**, *CYBERUK 2023 blog. Perspectives on change: AI ethics in the intelligence lifecycle*, Deloitte United Kingdom, 2023.

**O´Sullivan, M.** «Presentational Tradecraft: A New Skill», en Pherson, R. H., Arcos, R. (eds.): *Intelligence communication in the digital era: Transforming security, defence and business*, Palgrave Macmillan, Basingstoke, 2015.

**Páramo, A.**, «El analista de inteligencia de última generación», en Arteaga, F., Ríos Insúa, D. (coords.): *El analista de inteligencia en la era digital*, Real Instituto Elcano, Centro Nacional de Inteligencia, 2022.

**Pherson, R. H.**, **Arcos, R.**, *Intelligence communication in the digital era: Transforming security, defence and business*, Palgrave Macmillan, Basingstoke, 2015.

**Pyrik, J.**, «Communicating Risk», en Pherson, R. H., Arcos, R. (eds.): *Intelligence communication in the digital era: Transforming security, defence and business*, Palgrave Macmillan, Basingstoke, 2015.

**Rudin, C.**, *Four Principles of Explainable Artificial Intelligence*, National Institute of Standards and Technology (NIST), 2020.

**Serra del Pino, J.**, «Anticipando en tiempos postnormales», en Arteaga, F., Ríos Insúa, D. (coords.): *El analista de inteligencia en la era digital*, Real Instituto Elcano, Centro Nacional de Inteligencia, 2022.

**Stenslie, S., Haugom, L., Vaage, B. H.**, *Intelligence analysis in the digital age*, Routledge, Abingdon, 2021.

# LA ÉTICA COMO EJE TRANSVERSAL EN LA INTELIGENCIA

**Andrea Andreu Gutiérrez**
*Profesora e investigadora en formación (FPI)*
*Universidad de Valencia*

## 1. Introducción

En un Estado democrático de Derecho, incluso las actividades más sensibles, como son aquellas encomendadas a los servicios de inteligencia, deben llevarse a término con estricto respeto tanto a su normativa reguladora como a principios éticos que rigen su funcionamiento. En particular, haciendo especial mención a los servicios de inteligencia españoles —el Centro Nacional de Inteligencia[1]— con independencia de que las funciones que al mismo se encomiendan encuentran su fundamento en la defensa de la seguridad nacional, como desarrollaremos a lo largo del presente trabajo en ningún caso ello les habilita para actuar al margen del principio de legali-

1. Las funciones encomendadas al CNI, de conformidad con el art. 4 de la ley 11/2002, de 6 de mayo, consisten en: *«a) Obtener, evaluar e interpretar información y difundir la inteligencia necesaria para proteger y promover los intereses políticos, económicos, industriales, comerciales y estratégicos de España, pudiendo actuar dentro o fuera del territorio nacional. b) 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. c) Promover las relaciones de cooperación y colaboración con servicios de inteligencia de otros países o de Organismos internacionales, para el mejor cumplimiento de sus objetivos. d) Obtener, evaluar e interpretar el tráfico de señales de carácter estratégico, para el cumplimiento de los objetivos de inteligencia señalados al Centro. e) Coordinar la acción de los diferentes organismos de la Administración que utilicen medios o procedimientos de cifra, garantizar la seguridad de las tecnologías de la información en ese ámbito, informar sobre la adquisición coordinada de material criptológico y formar al personal, propio o de otros servicios de la Administración, especialista en este campo para asegurar el adecuado cumplimiento de las misiones del Centro. f) Velar por el cumplimiento de la normativa relativa a la protección de la información clasificada. g) Garantizar la seguridad y protección de sus propias instalaciones, información y medios materiales y personales».*

dad y del respeto a los derechos fundamentales recogidos en nuestra Norma Suprema; pues en todo caso deben desempeñar su labor con sometimiento pleno a la ley y al Derecho[2].

Como señala Pérez Luño, *«el constitucionalismo actual no sería lo que es sin los derechos fundamentales»* [3]. Ello implica que el respeto a los mismos se erige como principio inspirador de todo el sistema constitucional obligando tanto a los poderes públicos como al conjunto de la ciudadanía a garantizar y respetar la efectividad de aquéllos. En el ámbito que nos ocupa, los servicios de inteligencia deben llevar a cabo el desarrollo de sus funciones dentro de los límites que vienen impuestos del Estado de Derecho, con un régimen legal especial y sometiéndose en todo caso al debido control parlamentario y judicial previo, que legitime cualquier restricción de derechos[4].

En el ámbito español, la necesidad de ligar la ética a las funciones de inteligencia se ha puesto de manifiesto especialmente durante las últimas décadas, precisamente por la pérdida de legitimidad derivada de la sucesión de escándalos de gran magnitud sucedidos en el seno de los ya extintos servicios de inteligencia españoles (antiguo CESID) —como las escuchas telefónicas ilícitas que se produjeron durante las dos últimas décadas del siglo XX—. Aquellas interceptaciones ilegales de conversaciones privadas, muchas de ellas sin relevancia alguna para la defensa de la seguridad nacional, conllevaron la apertura de causas judiciales que involucraron a altos cargos de aquel organismo y suscitaron un escándalo público en torno a la vulneración de los derechos fundamentales por parte de los servicios de inteligencia estatales. Estos hechos evidenciaron la necesidad de configurar un marco ético-jurídico robusto que regulase el desarrollo de las labores de inteligencia para evitar que, en el futuro, volviesen a ocurrir situaciones similares. En este sentido, nuestro Tribunal Supremo afirmó poco después que ninguna razón de

2. Como dispone expresamente el apartado 1º del art. 2 de la ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia, relativo a los principios de actuación del mismo: *«El Centro Nacional de Inteligencia se regirá por el principio de sometimiento al ordenamiento jurídico y llevará a cabo sus actividades específicas en el marco de las habilitaciones expresamente establecidas en la presente Ley y en la Ley Orgánica 2/2002, de 7 de mayo, reguladora del control judicial previo del Centro Nacional de Inteligencia».*

3. Pérez Luño, A., *Los derechos fundamentales*, Tecnos, Madrid, 1988, pág. 19.

4. En este sentido, el art. 11 de la ley 11/2002, de 6 de mayo, relativo al control parlamentario, dispone lo siguiente: *«1. El Centro Nacional de Inteligencia someterá al conocimiento del Congreso de los Diputados, en la forma prevista por su Reglamento, a través de la Comisión que controla los créditos destinados a gastos reservados, presidida por el Presidente de la Cámara, la información apropiada sobre su funcionamiento y actividades. El contenido de dichas sesiones y sus deliberaciones será secreto (...)»* Por su parte, el artículo 12 (sobre el control judicial previo) establece: *«el control judicial previo del Centro Nacional de Inteligencia se llevará a cabo en la forma prevista en la Ley Orgánica reguladora del control judicial previo del Centro Nacional de Inteligencia, complementaria de la presente Ley».*

Estado prevalece sobre los preceptos de la Constitución que consagran los derechos fundamentales[5].

Fruto de todo ello, a comienzos de los años 2000 se aprobaron dos normas en el ámbito de los servicios de inteligencia españoles: por un lado, la Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia (que estableció la organización, el régimen jurídico, las funciones y actividades de la organización, entre otros aspectos) y, por otro lado, la Ley Orgánica 2/2002, de 6 de mayo, reguladora del control judicial previo del Centro Nacional de Inteligencia, que implementó un mecanismo de autorización judicial para las operaciones del servicio que pudieran conllevar alguna afectación de los derechos fundamentales a la inviolabilidad del domicilio o al secreto de las comunicaciones consagrados en los arts. 18.2 y 18.3 de la Constitución Española[6].

La finalidad esencial de las citadas normas, junto con las disposiciones del Código Ético del CNI que se aprobaría unos años después, en 2015, fue precisamente tratar de garantizar que el desarrollo de las funciones encomendadas a este organismo se llevase a cabo con las máximas garantías y de acuerdo con las exigencias del Estado de Derecho quedando sometido a un riguroso control parlamentario y judicial, cubriendo además las carencias que en el pasado habían situado ciertas prácticas en una suerte de limbo que desembocaron en multitud de excesos y actuaciones irregulares. Ahora bien, con el paso del tiempo, la suficiencia de este marco normativo se ha puesto en entredicho y ha sido objeto de numerosas críticas y propuestas de mejora[7].

Autores como Revenga Sánchez han calificado estas disposiciones como *«un corpus normativo superficial y elaborado con urgencia para apaciguar las voces críticas que se hacían oír con relación a lo ocurrido en el CESID, pero también con respecto a todo lo que se hizo al margen de la ley para enfrentar el terrorismo, incluido el descontrol y el saqueo de los llamados desde entonces fondos reservados»*. Este autor señala además que *«el diseño de los controles parlamentario y judicial era todo un modelo de improvisación y superficialidad»*, si bien constituyó un avance inicial imprescindible[8].

---

5. Lozano Cutanda, B., «La desclasificación de los secretos de Estado», Revista de administración pública, núm. 146, 1998, págs. 524-529.

6. De acuerdo con el mencionado precepto constitucional: *«2. El domicilio es inviolable. Ninguna entrada o registro podrá hacerse en él sin consentimiento del titular o resolución judicial, salvo en caso de flagrante delito. 3. Se garantiza el secreto de las comunicaciones y en especial, de las postales, telegráficas y telefónicas, salvo resolución judicial».*

7. Como ha defendido un amplio sector doctrinal, la ley reguladora del funcionamiento del Centro Nacional de Inteligencia destaca por su imprecisión y ambigüedad. Por otro lado, también podemos hacer referencia, como aspecto cuanto menos llamativo, la brevedad del texto que sirve de desarrollo a esta disposición legal, la LO 2/2002, de 6 de mayo, reguladora del control judicial previo del Centro Nacional de Inteligencia, la cual consta de un único precepto.

8. Revenga Sánchez, M., «El control del Centro Nacional de Inteligencia: una perspectiva comparada. *Revista Española de Derecho Constitucional»,* nº 116*,* 2019*,* págs. 13-47.

## 2. El concepto de inteligencia y su dimensión ética

Tras haber expuesto en líneas anteriores los antecedentes de la actual normativa en materia de servicios de inteligencia en España y las exigencias de implementar la citada regulación, a continuación delimitaremos el sentido y alcance del término *«inteligencia»* circunscrito al ámbito de la seguridad nacional y el lugar y la importancia que ocupa en el seno de un Estado democrático de Derecho, como es el nuestro.

Tradicionalmente, este concepto ha estado íntimamente ligado a la producción de conocimiento relevante para la toma de decisiones gubernamentales en materia de defensa y seguridad. En este sentido, Sherman Kent ofreció por vez primera una definición de *«inteligencia»* en 1949, haciendo referencia tanto al conocimiento para la toma de decisiones por parte del Gobierno, como a la disciplina de Estudios de Inteligencia. En este sentido, sostuvo que: *«inteligencia es el conocimiento en el que los decisores civiles y militares deben basar sus decisiones con el fin de salvaguardar los intereses internacionales y el bienestar de la nación, suministrado por unos organismos que recogen y analizan información denominados servicios de inteligencia»*[9].

Sin embargo, como señalan Esteban Navarro y Carvalho, *«los ámbitos de acción de la inteligencia se han ampliado a lo largo de las tres últimas décadas de la mano de fenómenos tan variados como la evolución del concepto de seguridad, la aparición de nuevos riesgos y amenazas, la expansión de su práctica por múltiples instituciones del Estado, la incorporación de las empresas como productoras y beneficiarias de inteligencia para el desarrollo de negocios y la obtención de beneficios mercantiles (...) o la progresiva participación de compañías privadas en la producción de inteligencia gubernamental. Estas transformaciones han modificado e incrementado los actores de la inteligencia, tanto de sus productores como de sus usuarios, los asuntos de que se ocupa, las técnicas que se utilizan, la colaboración nacional e internacional en su producción y compartición, las normas jurídicas y éticas que la regulan, la relación del mundo de la inteligencia con la sociedad y su imagen pública»* [10].

De este modo, podemos afirmar pues, que la inteligencia implica un valor añadido a la mera información dado que esta misma integra datos dispersos, los contextualiza y permite extraer conclusiones que orientan la toma de decisiones estratégicas de un Estado. En este sentido, estos mismos autores definen la inteligencia como *«la culminación del proceso de utilización de conocimiento tácito y explícito pertinentes para analizar y evaluar un determinado objetivo, con el fin de alinear decisiones y acciones adecuadas para aprovechar oportunidades o contrarrestar amenazas. En otras palabras, la inteligen-*

9. Kent, S., *Strategic Intelligence for American World Policy*, Princeton University Press, 1949.

10. Esteban Navarro M. A., Carvalho, A. V., «La inteligencia y los activos informacionales» en González Cussac, J. L. (Coord.): *Inteligencia,* Tirant lo Blanch, 2012, págs. 19 y ss.

*cia consiste en el empleo de la información y el conocimiento más adecuados para atender a una necesidad específica orientada a la toma de decisiones y a la acción por parte de un determinado individuo o grupo»*[11]*.* Así pues, podríamos afirmar que, de acuerdo con dicha definición, la materia prima de la inteligencia es la información obtenida a través de diversas fuentes, convertida en conocimiento útil mediante la aplicación de rigurosos métodos analíticos.

Ahora bien, en una sociedad democrática, la actividad de inteligencia no solo se evalúa por su eficacia para descubrir potenciales amenazas, sino también por el modo en que la misma se desarrolla; esto es, por su adecuación a determinados valores o principios éticos que deben estar presentes en todas las fases del denominado *«ciclo de inteligencia»*[12] garantizando que cada actuación se ajuste a unos estándares de corrección y respeto a la dignidad humana y al ordenamiento jurídico. El marco normativo español configura explícitamente esta exigencia ética. De hecho, la Constitución Española proclama en su artículo 10.1 que *«la dignidad de la persona, los derechos inviolables que le son inherentes, el respeto a la ley y a los derechos de los demás, son fundamento del orden político y de la paz social»,* sentando así una base que sirve de eje para el desarrollo de las funciones de inteligencia y, por otro lado, el artículo 9.1 CE dispone expresamente que *«los ciudadanos y los poderes públicos están sujetos a la Constitución y al resto del ordenamiento jurídico».*

Una vez sentado lo anterior, debemos prestar especial atención a un elemento esencial en el marco normativo, que viene constituido por el binomio *«seguridad-libertad»*[13]*.* Lejos de concebirse como conceptos contrapuestos, la libertad y la seguridad deben interpretarse como valores complementarios, de tal modo que la seguridad del Estado pueda quedar suficientemente

---

11. Esteban Navarro M. A., Carvalho, A. V., «La inteligencia y los activos informacionales» *(op. cit.),* pág. 25.

12. Como señala López Temporal, *«el llamado ciclo de inteligencia consta de cuatro etapas inicialmente independientes y complementadas entre sí. Es la secuencia mediante la cual: se obtiene información, se transforma en inteligencia y se pone a disposición de los usuarios esta inteligencia (...) La esencia de este ciclo es conseguir inteligencia, definida como el producto que resulta de la valoración, análisis, integración e interpretación de la información reunida por un servicio de inteligencia»;* López Temporal, V. M., «La investigación policial en los delitos de criminalidad organizada» en González Cussac, J. L., Cuerda Arnau, M. L. (dir.), Fernández Hernández, A. (coord.): *Nuevas amenazadas a la Seguridad Nacional*, Tirant lo Blanch, 2013, pág. 365.

13. En palabras de Orts Berenguer, *«libertad y seguridad no son incompatibles, como se cree o se pretende hacer creer por algunos o por muchos, no aumenta una porque disminuya la otra (salvo para los dictadores y su círculo fiel), al contrario, se complementan. El pacto social en cuyo marco vivimos tiene por objeto el logro de una convivencia segura y en libertad. Y esto sólo es posible en un Estado de Derecho que, con todas sus imperfecciones, es el único que respeta la dignidad del ser humano, al tratarle, con arreglo a la idea kantiana, como sujeto y no como objeto, y el único que nos ampara a todos frente a las extralimitaciones de los poderes públicos».*
Orts Berenguer, E., «Presentación. A propósito de la seguridad», en Orts Berenguer (et.al.): *Sobre la Ciencia de la Seguridad,* Tirant lo Blanch, págs. 15 y ss.

garantizada respetando la efectividad de los derechos y libertades fundamentales y, en todo caso, debiendo preservar su contenido esencial. En esta línea, nuestro Tribunal Constitucional ha afirmado en diversas ocasiones que los derechos fundamentales pueden tener límites, si bien los mismos no pueden revestir carácter general sino específico, venir configurados por una norma con rango de ley y estar sujetos al pertinente control judicial para garantizar su legitimidad.

En términos prácticos, todo ello se traduce en que cualquier actuación o medida que se adopte en materia de inteligencia y que pudiera interferir de algún modo en el ejercicio de los derechos fundamentales, deberá estar contemplado con carácter previo en una ley que defina los presupuestos habilitantes, los límites y las condiciones para poder llevar a cabo dicha injerencia. La jurisprudencia española ha establecido que resulta esencial para llevar a cabo cualquier injerencia o intervención sobre el derecho al secreto de las comunicaciones, respetando en todo caso el contenido esencial del mismo[14]. En este sentido, el Tribunal Supremo ha admitido en numerosas ocasiones las interceptaciones como prueba en un proceso, bien para evidenciar la comisión de un delito o para el descubrimiento de sus responsables. Dicho lo cual, el Tribunal Constitucional ha previsto que la autorización judicial para llevar a cabo la intervención debe dictarse en el seno del proceso de que se trate[15]. Estos pronunciamientos ponen de manifiesto la necesidad de dotar de cobertura legal a las operaciones de inteligencia, debiendo seguir cauces reglados para la ejecución de actividades intrusivas. Como avanzábamos, todo ello desembocó en la elaboración de diversas normas durante el año 2002, y que configuran hoy el marco jurídico básico de los servicios de inteligencia en España.

Además, pese a que cada país dentro de la Unión Europea posee diferentes realidades y necesidades a nivel de seguridad nacional frente a las amenazas a las que se enfrente, a estas nuevas normas se podría en un futuro incorporar, tal y como señala González López, *«la existencia de un sistema integrado de inteligencia europeo que fuese capaz de generar información útil, pertinente y elaborada para la toma de decisiones por sí mismo, es decir, capaz de realizar*

14. En palabras de Aba Catoira, «*Respecto a las intervenciones en el secreto de las comunicaciones, la jurisprudencia constitucional se ha mostrado intransigente no cediendo en la necesidad de contar con la autorización judicial. En orden a la limitación de derechos, la Constitución establece en el art. 53.1 la reserva de ley, y la autorización judicial expresamente en el ámbito del 18.3, por lo que cabría sostener que no son requisitos que hayan de cumplimentarse a la vez como garantía del derecho, siendo suficiente con uno de ellos. Es decir, una ley podría prever la posibilidad de limitación sin necesidad de la autorización judicial por razones de seguridad nacional, lo que estaría en línea con las justificaciones que amparan las intervenciones en el ámbito del 18.2. (...) No obstante, la jurisprudencia del Tribunal Europeo de Derechos Humanos refuerza la exigencia de autorización judicial para proceder aunque lo haga indirectamente*»; Aba Catoira, A., «El secreto de Estado y los servicios de inteligencia», *Cuadernos Const. De la Cátedra Fadrique Furió Ceriol nº 38/39,* Valencia, 2002*,* pág. 165.

15. Sentencia del Tribunal Constitucional 49/1999, de 5 de abril (ECLI:ES:TC:1999:49)

*el ciclo de inteligencia»* para conformar un cuerpo normativo e institucional adaptado a las exigencias de los nuevos escenarios internacionales[16].

La Exposición de Motivos de la ley 11/2002 establece que *«el Centro Nacional de Inteligencia sustituye al Centro Superior de Información de la Defensa (...) La principal misión del Centro Nacional de Inteligencia será la de proporcionar al Gobierno la información e inteligencia necesarias para prevenir y evitar cualquier riesgo o amenaza que afecte a la independencia e integridad de España, los intereses nacionales y la estabilidad del Estado de derecho y sus instituciones. El Centro continuará adscrito al Ministerio de Defensa. Sus objetivos, definidos por el Gobierno, serán aprobados anualmente por el Consejo de Ministros y se plasmarán en la Directiva de Inteligencia. El Centro Nacional de Inteligencia funcionará bajo el principio de coordinación con los demás servicios de información del Estado español».*

Una vez sentado lo anterior, y sin perjuicio de ser desarrollado con mayor detenimiento en el epígrafe siguiente, haremos una breve mención a los principios básicos que deben guiar el desarrollo de las funciones de inteligencia para garantizar la ética en este ámbito. Se trata principalmente de los siguientes:

El principio de legalidad, ya mencionado anteriormente, supone que toda acción de inteligencia debe estar amparada por normas jurídicas positivas (y si afectan derechos fundamentales, bajo reserva de Ley Orgánica de conformidad con el art. 81.1 CE)[17]. Por otro lado, los principios de necesidad y proporcionalidad conllevan que las medidas de obtención de información que restrinjan derechos deberán ser estrictamente necesarias para la consecución de un objetivo legítimo de seguridad y guardar una proporción adecuada entre la intrusión que suponen y la gravedad de la amenaza que se trate de prevenir [18].

En relación con los principios de responsabilidad y control, se trata de aquellos que imponen a los servicios de inteligencia la obligación de rendir cuentas de sus actividades ante los organismos competentes en cada caso. Por último, los principios de integridad y ética profesional, así como el respeto a la dignidad humana, entre otros, proscriben taxativamente la utilización de métodos lesivos para la integridad de las personas en todo caso. De este conjunto de principios se desprende que la inteligencia estatal no puede

16. González López, D., «La integración europea en materia de inteligencia: ¿un servicio de inteligencia europeo?», *Studia Humanitatis Journal, 2024*, vol. 4, núm. 2, pág. 18.

17. Como dispone el citado artículo: *«1. Son leyes orgánicas las relativas al desarrollo de los derechos fundamentales y de las libertades públicas, las que aprueben los Estatutos de Autonomía y el régimen electoral general y las demás previstas en la Constitución»*.

18. Como señala González López, *«en los Estados de Derecho (...) toda actividad de inteligencia debe ejecutarse bajo principios de legitimidad y eficacia. La legitimidad implica el sometimiento estricto a la Constitución, a las leyes y reglamentos nacionales, mientras que la eficacia requiere una adecuada proporcionalidad entre los medios empleados y los fines perseguidos»*; González López, D., «La influencia de la inteligencia en el Derecho penal internacional», *ReCrim. Revista de l'Institut Universitari d'Investigació en Criminologia i Ciències Penals de la UV,* núm. 33, 2025, pág. 71.

concebirse como un poder excepcional al margen de la ética y la ley, sino precisamente como una actividad cuya legitimidad deriva de su adhesión a los principios y valores democráticos.

## 3. Principios rectores de las actividades de inteligencia

Como avanzábamos en líneas anteriores, a lo largo del presente epígrafe procederemos a desarrollar con mayor detenimiento algunos de los principios esenciales que deben guiar la actuación de los servicios de inteligencia en nuestro país. Dichos principios tienen una doble significación: pues no solamente se encuentran expresamente recogidos y positivizados en la normativa que regula el ámbito que nos ocupa, sino que también se erigen como valores deontológicos y éticos que sirven de guía en materia de inteligencia y seguridad.

En primer lugar, debemos hacer referencia al principio de legalidad, de conformidad con el cual el desarrollo de las labores de inteligencia debe realizarse con plena sujeción a la Constitución y al resto del ordenamiento jurídico. Este principio, reflejado en los arts. 9.1 y 103.1 CE, entre otros, supone que cada actuación debe encontrar cobertura normativa de acuerdo con la legislación vigente en el momento de que se trate. Concretamente, la ley 11/2002, de 6 de mayo, establece en su art. 2, relativo a los principios de actuación del CNI, que *«1. El Centro Nacional de Inteligencia se regirá por el principio de sometimiento al ordenamiento jurídico y llevará a cabo sus actividades específicas en el marco de las habilitaciones expresamente establecidas en la presente Ley y en la Ley Orgánica 2/2002, de 6 de mayo, reguladora del control judicial previo del Centro Nacional de Inteligencia».*

En segundo lugar, el respeto a los derechos fundamentales exige que ninguna actividad en materia de inteligencia pueda afectar a los mismos, salvo en la medida en que una norma de rango suficiente autorice una limitación concreta y proporcionada. Ello conlleva dos consecuencias: en primer lugar, que los servicios de inteligencia deberán velar por el respeto a los derechos fundamentales en el ejercicio de sus funciones y optar, en la medida de lo posible, por la utilización de los métodos menos gravosos a su alcance y, por otro lado, que, incluso cuando se produzca la limitación de un derecho de acuerdo con el principio de proporcionalidad, en ningún caso podrá quedar afectado su contenido esencial. Así, por ejemplo, el CNI podría intervenir determinadas comunicaciones privadas por motivos de seguridad nacional, pero en ningún caso estaría legitimado para llevar a cabo actuaciones que vacíen de contenido el derecho al secreto de las comunicaciones[19].

19. Como recuerda Martínez Galindo en relación a la intervención de las comunicaciones telefónicas y el deber de motivación, el TC ha afirmado en numerosas ocasiones que *«La resolución judicial que acuerda una intervención telefónica ha de justificar la existencia de los presupuestos materiales habilitantes de la intervención: los datos objetivos que puedan*

En este sentido, el Tribunal Constitucional ha puesto de manifiesto que el ejercicio de la seguridad no puede menoscabar la vigencia de los derechos fundamentales, los cuales mantienen su valor preferente en nuestro ordenamiento. De hecho, la posible colisión entre *«seguridad y libertad»* [20] a la que nos hemos referido en páginas anteriores, deberá resolverse mediante la correspondiente ponderación en el caso concreto, debiendo tener presente que toda afectación o restricción deberá quedar suficientemente justificada o motivada, así como ser objeto de control y revisión en los términos legalmente previstos. En consecuencia, el respeto a los derechos fundamentales no puede quedar subordinado a consideraciones de eficacia, sino que del mismo depende la legitimidad de los servicios de inteligencia.

En tercer lugar, también debemos hacer referencia a los principios de necesidad, idoneidad y proporcionalidad, que resultan de aplicación a las medidas de inteligencia que conlleven incidencia en los derechos de las personas. El principio de necesidad implica, en términos generales, que tan solo se deberán adoptar medidas extraordinarias en tanto en cuanto resulten estrictamente imprescindibles para lograr la finalidad de que se trate; esto es, cuando no existan medios menos lesivos para obtener la información requerida. Por otro lado, el principio de idoneidad exige que la medida aplicada deberá resultar adecuada para la consecución del objetivo propuesto en el caso concreto.

Por su parte, el principio de proporcionalidad requerirá la apreciación de un equilibrio justo entre la intensidad de la injerencia en el derecho de que se trate y la relevancia del interés público que se persigue; esto es, que la afec-

*considerarse indicios de la posible comisión de un hecho delictivo grave y de la conexión de las personas afectadas por la intervención con los hechos investigados. Indicios que son algo más que simples sospechas, pero también algo menos que los indicios racionales que se exigen para el procesamiento (...) si el secreto pudiera alzarse sobre la base de meras hipótesis subjetivas, el derecho al secreto de las comunicaciones, tal y como la CE lo configura, quedaría materialmente vacío de contenido»* (entre otras: STC 197/2009, de 28 de septiembre. Recurso de amparo núm. 891/2007. Ponente: D. Javier Delgado Barrio); Véase Martínez Galindo, G: «Jurisprudencia del Tribunal Constitucional», *Anuario de Derecho Penal y Ciencias Penales,* núm. 63, 2010.

20. Como señala Velasco Fernández, *«no se trata ya de tener que escoger entre libertad o seguridad. Ni con aquellos que creen que se puede conseguir vivir en libertad sin seguridad porque son unos ingenuos peligrosos, ni con aquellos que renuncian a la libertad sólo por tener seguridad porque son prescindibles. ¿Por qué no complementar ambas dimensiones para hacer de ellas una situación más habitable para los ciudadanos? No se trata de que una anule a la otra. Se pretende que la seguridad sea la suficiente para elevar la libertad a los máximos niveles posibles. La seguridad que se acepta, en lugar de coartar las libertades, las garantiza y las refuerza sabiendo que nunca se está seguros del todo ni nunca se es libre de forma absoluta. (...) Es la ética de la complementariedad lo que lleva a considerar que si las razones que tiene un servicio de inteligencia a la hora de realizar algo son por un lado, una buena razón, y por otro, la verdadera razón, ambas se tienen que complementar»;* Véase Velasco Fernández, F.: «Ética» en Díaz Fernández, A. M. (dir.): *Conceptos Fundamentales de Inteligencia*, Tirant lo Blanch, 2016.

tación al derecho fundamental no revista carácter desmedido en comparación con el beneficio que se espera obtener en términos de seguridad. Este último aparece expresamente plasmado en el artículo 17 del Código Ético del CNI, de conformidad con el cual: *«quienes sirven en el Centro Nacional de Inteligencia se responsabilizarán de que la utilización de los procedimientos especiales que permite la ley guarde siempre la debida proporcionalidad, en función del riesgo o amenaza que se pretenda combatir o del conocimiento que se desee obtener»*[21].

En cuarto lugar, también debemos mencionar los principios de control y responsabilidad[22]: la rendición de cuentas constituye un componente ético esencial en la gestión de inteligencia. Dado el carácter reservado de las actividades del CNI, deviene de todo punto imprescindible que existan mecanismos de control interno y externo que aseguren que el servicio no se desvíe de la legalidad ni de la ética[23].

En relación con las exigencias derivadas de los principios de integridad, honestidad y lealtad institucional, la integridad implica que el personal al servicio de estos organismos actúe evitando la comisión de cualquier práctica irregular, la utilización abusiva de información o el aprovechamiento de su posición para la satisfacción de sus intereses particulares, entre otras conductas[24]. La lealtad institucional implica, por su parte, que el personal de inteligencia deberá anteponer los intereses generales y la seguridad del Estado en el desempeño de sus funciones, frente a motivaciones de cualquier otra índole[25].

---

21. De ello se deriva que toda actuación llevada a cabo por los servicios de inteligencia debe ser evaluada de acuerdo con las exigencias del principio de proporcionalidad, el cual puede considerarse como imperativo ético en el desarrollo ordinario de las funciones de este organismo.

22. Señala Boltaina Bosch que *«las normas reguladoras del personal al servicio de la inteligencia han debido adoptar regulaciones específicas en muy variadas cuestiones, para armonizar e interrelacionar la especial función de inteligencia del poder público con los derechos y obligaciones de los empleados que las desarrollan. (...) Las normas han ido progresivamente incorporando un corpus normativo de deberes, pero muy especialmente de derechos, paralelo al existente para el personal civil, policial o militar. Destacan especialmente los principios de igualdad, mérito y capacidad, (...) formación permanente o evaluación y responsabilidad en las funciones»*; Véase Boltaina Bosch, X., «Estatuto de personal» en Díaz Fernández, A. M. (dir.): *Conceptos Fundamentales de Inteligencia,* Tirant lo Blanch, 2016.

23. Ello encuentra reflejo en el art. 8 de su Código Ético, el cual dispone entre sus principios, que *«con sentido de la responsabilidad, aceptarán las consecuencias de su actuación, adoptarán con firmeza las decisiones que les correspondan y asumirán con honradez cuanto de ellas se derive».*

24. El Código Ético del CNI recoge muchos de estos valores. proclama en su art. 12 que *«la honradez será un principio rector, tanto de su comportamiento personal como de su actuación profesional»*, instando a que los miembros del CNI se conduzcan en todo momento de manera íntegra y digna.

25. Íntimamente relacionado con lo expuesto, nos remitimos a lo dispuesto en el art. 6 del Código Ético, relativo a los principios de objetividad e imparcialidad.

Respecto al deber de reserva, una característica particular de la ética de la inteligencia se manifiesta en la importancia que reviste la confidencialidad. Como pone de manifiesto Boltaina Bosch, *«mención especial merece el requerimiento a los empleados de inteligencia de un compromiso ético y de conducta y profesional muy riguroso, que oscila en función de cada país. Estos elementos se concretan especialmente en: (...) la existencia de un intenso deber de secreto y deber de reserva profesional. Ambos deberes se articulan de manera por lo general extensísima y su incumplimiento implica una responsabilidad disciplinaria y/o penal, que se prolonga más allá de la finalización de los servicios profesionales, al ser considerado una condición sine qua non imprescindible para una completa confianza entre y con el personal (caso Attorney-General vs. Blake, 2000, Reino Unido) y recogida en todas las nuevas leyes de inteligencia de las últimas décadas»* [26]. En este sentido, la ley 11/2002 también hace especial referencia al secreto al regular las actividades encomendadas al CNI[27].

En último lugar, el principio de servicio a la sociedad y primacía del interés general conlleva que la ética de la inteligencia española debe considerarse un servicio público cuyo objetivo esencial reside en contribuir a la consecución del bien común: la libertad, la seguridad y la justicia en la sociedad[28].

Los principios expuestos conforman una suerte de código moral y jurídico que debe guiar toda actuación de los servicios de inteligencia. No se trata tan solo de meros postulados teóricos o filosóficos sino que, como hemos visto, todos ellos han sido efectivamente positivizados en distintas normas reguladoras del desarrollo de las tareas de inteligencia por parte de los organismos competentes y evidencian la importancia otorgada a la ética como parte intrínseca de la profesión de inteligencia en España.

---

26. Boltaina Bosch, X., «Estatuto de personal» en Díaz Fernández, A. M. (dir.): *Conceptos Fundamentales de Inteligencia,* Tirant lo Blanch, 2016, págs. 163-164

27. Como dispone el art. 5 de la norma, relativo a las actividades del Centro Nacional de Inteligencia: *«1. Las actividades del Centro Nacional de Inteligencia, así como su 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, constituyen información clasificada, con el grado de secreto, de acuerdo con lo dispuesto en la legislación reguladora de los secretos oficiales y en los Acuerdos internacionales o, en su caso, con el mayor nivel de clasificación que se contemple en dicha legislación y en los mencionados Acuerdos».*

28. De hecho, el Código Ético del CNI concluye afirmando en su artículo 20, relativo al servicio a España, que *«Todos los miembros del Centro Nacional de Inteligencia asumirán como valores consustanciales al servicio a España en el Centro la profesionalidad, la integridad y el rigor, el sentido del compromiso, la discreción, el espíritu de sacrificio, la lealtad, el respeto a jefes, compañeros y subordinados, el trabajo en equipo, la altura de miras y la búsqueda de la excelencia».*

## 4. Jurisprudencia relevante en la materia

La jurisprudencia española se ha encargado en numerosas ocasiones de delimitar los límites éticos y jurídicos a que deben quedar sometidas las actividades llevadas a cabo por los servicios de inteligencia, especialmente en lo que respecta a la garantía y efectividad de los derechos fundamentales de la ciudadanía, frente a posibles injerencias en los mismos. Estos pronunciamientos se erigen como principios de alcance general que orientan la actuación y desarrollo de las funciones encomendadas al Centro Nacional de Inteligencia y los poderes públicos en este ámbito.

Haciendo expresa referencia a algunos de los pronunciamientos más importantes como apunta la Sentencia del Tribunal Constitucional 49/1999, de 5 de abril[29], FJ 6, en relación al secreto de las comunicaciones: *«La garantía jurisdiccional del secreto de las comunicaciones no se colma con su concurrencia formal -autorización procedente de un órgano jurisdiccional- sino que ésta ha de ser dictada en un proceso, único cauce que permite hacer controlable, y con ello jurídicamente eficaz, la propia actuación judicial. La naturaleza de la intervención telefónica, su finalidad y la misma lógica de la investigación exigen que la autorización y desarrollo de la misma se lleve a cabo, inicialmente, sin conocimiento del interesado, que tampoco participa en su control. Sin embargo, al desarrollarse la actuación judicial en el curso de un proceso, esta ausencia ha de suplirse por el control que en él ejerce el Ministerio Fiscal, garante de la legalidad y de los derechos de los ciudadanos ex art. 124.1 C.E., y posteriormente, cuando la medida se alza, el propio interesado ha de tener la posibilidad, constitucionalmente necesaria dentro de ciertos límites que no procede precisar aquí, (Sentencia del T.E.D.H., caso Klass, núm. 55), de conocer e impugnar la medida».*

Por su parte, en otras resoluciones, como la Sentencia del Tribunal Constitucional 55/1996, de 28 de marzo[30], el Tribunal Constitucional ha hecho expresa mención al principio de proporcionalidad en esta sede, teniendo en cuenta la finalidad perseguida y los medios utilizados. De acuerdo con la mencionada resolución: *«El ámbito en el que normalmente y de forma muy particular resulta aplicable el principio de proporcionalidad es el de los derechos fundamentales. Así ha venido reconociéndolo este Tribunal en numerosas Sentencias en las que se ha declarado que la desproporción entre el fin perseguido y los medios empleados para conseguirlo puede dar lugar a un enjuiciamiento desde la perspectiva constitucional cuando esa falta de proporción implica un sacrificio excesivo e innecesario de los derechos que*

29. ECLI:ES:TC:1999:49

30. ECLI:ES:TC:1996:55

*la Constitución garantiza (SSTC* 62/1982[31]*, FJ 5º;* 66/1985[32]*, FJ 1º;* 19/1988[33]*, FJ 8º;* 85/1992[34]*, FJ 5º;* 50/1995[35]*, FJ 7º).*»

En relación con los límites correspondientes al secreto y la realización de un juicio de ponderación, no podemos dejar de hacer referencia a las sentencias dictadas por el Tribunal Supremo en 1997. Como pone de relieve Garrido Cuenca, *«la cuestión medular de estas resoluciones residía en determinar los límites de la potestad jurisdiccional para revisar la decisión del Consejo de Ministros de no desclasificar los documentos declarados secretos en un espacio de «ponderación y compaginación de intereses constitucionales que en apariencia se revelan como de difícil conciliación»: la protección de la seguridad del Estado y el derecho a la tutela judicial efectiva. El conflicto se produce ante los sucesivos requerimientos del juez de instrucción, primero al CESID (por siete veces), después al Ministerio de Defensa, para la entrega de diversos documentos relativos a la supuesta guerra sucia contra ETA, organización del GAL, información sobre determinados altos cargos del Ministerio de Interior y estructura de los archivos del CESID. El director del Centro reiteró en todas y cada una de las ocasiones el carácter secreto de las informaciones, documentos y datos obrantes en el CESID, así como el deber de secreto que la legislación de secretos oficiales impone al Centro. (...) Finalmente se dictaron tres sentencias, todas de 4 de abril de 1997* [36] *en las que se declara la nulidad parcial del acuerdo del Consejo de Ministros que denegó la desclasificación de los documentos requeridos judicialmente, ordenándose al Gobierno la cancelación como reservados de 18 de los documentos solicitados»* [37].

De todo ello, podemos extraer varias conclusiones importantes: en primer lugar, que el desarrollo de las actividades por parte de los servicios de inteligencia pueden ser objeto de control judicial y conllevar la asunción de responsabilidad en aquellos casos en que se produzca la vulneración de derechos; en segundo lugar, que incluso aquellas materias constitutivas de secreto oficial se encuentran sujetas a determinados límites, de tal modo que no puede esgrimirse con la finalidad de obstaculizar una investigación judicial. En este sentido, el Tribunal Supremo esgrimió que la Ley 9/1968, de 5 de

31. Sentencia 62/1982, de 15 de octubre (ECLI:ES:TC:1982:62)

32. Sentencia 66/1985, de 23 de mayo (ECLI:ES:TC:1985:66)

33. Sentencia 19/1988, de 16 de febrero (ECLI:ES:TC:1988:19)

34. Sentencia 85/1992, de 8 de junio (ECLI:ES:TC:1992:85)

35. Sentencia 50/1995, de 23 de febrero (ECLI:ES:TC:1995:50)

36. Fueron ponentes los magistrados Trillo Torres (en el caso Oñederra), Cáncer Lalanne (en el caso Urigoitia) y Lescure Martín (en el caso Lasa-Zabala).

37. Garrido Cuenca, N., «El episodio judicial de la desclasificación de los papeles del CESID: las sentencias del Tribunal Supremo de 4 de abril de 1997. Paradojas y paralogismos de un conflicto entre la función de gobierno y el derecho a la tutela judicial efectiva», *Revista de Administración Pública,* núm. 143, 1997, págs. 229 y ss.

abril, sobre secretos oficiales, debía interpretarse de modo respetuoso con el derecho a la tutela judicial efectiva (art. 24 CE). Por último, que toda actividad de inteligencia debe desarrollarse en el marco de los límites y principios constitucionales y legales, quedando sometidos al principio de legalidad y pleno sometimiento al ordenamiento jurídico.

En base a todo ello, como vemos la jurisprudencia española ha afirmado taxativamente que los servicios de inteligencia no pueden operar en una suerte de vacío normativo, sino bajo las exigencias derivadas del Estado de Derecho, sin que por ello quede mermada la eficacia del funcionamiento de aquellos. El Tribunal Constitucional, por su parte, también ha hecho hincapié en la necesidad de respetar los principios de legalidad, necesidad, proporcionalidad, excepcionalidad y control previo a la hora de llevar a cabo la afectación o restricción de derechos por motivos de seguridad, para evitar abusos y excesos que pudieran cometerse en pro de la seguridad.

## 5. Conclusiones

A lo largo del presente trabajo hemos puesto de manifiesto que la ética se erige como eje vertebrador que debe guiar el desarrollo de las actividades encomendadas a los servicios de inteligencia en el marco de un Estado de Derecho. En el caso de España, estos agentes, a fin de preservar y garantizar la seguridad nacional frente a posibles amenazas, deben quedar sometidos en todo caso a las exigencias derivadas del principio de legalidad y el respeto a la dignidad de las personas para conservar la legitimidad y la confianza de la ciudadanía en su funcionamiento.

De este modo, la necesidad de sujetar su actuación a determinados principios, como son los de legalidad, proporcionalidad, integridad, control y responsabilidad, entre otros, resulta imprescindible para garantizar la transparencia de estos organismos y para evitar la comisión de irregularidades y la vulneración sistemática de derechos, tal y como ocurrió en el seno del antiguo CESID a finales del siglo XX. Precisamente por ello, actualmente en España se ha consolidado un amplio marco normativo que garantiza el sometimiento de los servicios de inteligencia a estrictos procedimientos y principios éticos y deontológicos y su actuación es rigurosa, responsable, objetiva y honesta o, al menos, debería serlo.

Además, ya no solo las normas positivas, sino también numerosos pronunciamientos jurisprudenciales en la materia han puesto de manifiesto durante los últimos años los límites taxativos a que se encuentran sometidos los servicios de inteligencia, recordando que el fin no justifica los medios si los mismos conllevan la vulneración de derechos constitucionalmente consagrados. Todo ello contribuye pues, a configurar un escenario en el cual la ética debe estar presente en el funcionamiento ordinario de los servicios de inteligencia en España: tanto en materia de planificación de objetivos, como en la obtención

de información (mediante la utilización de métodos y procedimientos legítimos), el tratamiento de los datos (de conformidad con la normativa en materia de protección de datos) y la difusión de la información obtenida.

Con todo, no es menos cierto que durante los últimos años hemos asistido a la irrupción de nuevas realidades que plantean cuestiones problemáticas en la materia: así, entre otras, la aparición de nuevas tecnologías de vigilancia masiva o la inteligencia artificial aplicada a seguridad, que despiertan dudas sobre la aplicación de los principios de proporcionalidad y control. Frente a todas estas nuevas amenazas, tal y como hemos indicado, por ejemplo, en relación con la posible creación de un sistema integrado de inteligencia europeo, los Estados deben actuar para garantizar la seguridad considerando la ética como eje transversal de los servicios de inteligencia para garantizar legitimidad, legalidad y eficacia duradera en la protección de los derechos de sus ciudadanos.

Así, las funciones de inteligencia deben descansar en una serie de principios éticos y jurídicos que inspiren toda su actuación: legalidad (todas las actuaciones deben venir expresamente previstas en una norma con rango de ley, o, en su caso, de ley orgánica si conlleva la afectación de derechos fundamentales); necesidad y proporcionalidad (mediante la aplicación de aquellas medidas estrictamente imprescindibles para la consecución de los fines legítimos de seguridad y optando por los medios menos lesivos posibles), responsabilidad y control (esto es, la obligación de rendir cuentas ante los órganos parlamentarios y judiciales en los términos legalmente previstos), integridad y servicio al interés general (debiendo estar orientadas las labores de inteligencia a la consecución de intereses generales). El cumplimiento de estos principios se erige como la base sobre la que se asienta la legitimidad de la actividad de inteligencia en una sociedad democrática.

Por último, y como propuesta de *lege ferenda*, tras lo expuesto, sería tal vez interesante implementar algunas medidas tendentes a la introducción de mejoras en el marco normativo e institucional en materia de inteligencia y seguridad. Así, por ejemplo, fortalecer los mecanismos de control y supervisión sobre el personal integrante del Centro Nacional de Inteligencia, fomentar la transparencia en la medida en que ello resulte compatible con la preservación de la seguridad, así como potenciar la formación de sus integrantes en estos valores, con la finalidad de lograr llegar a un consenso sobre el equilibrio entre seguridad y libertad. Mediante la puesta en marcha de estas medidas, debería llegar a reforzarse la legitimidad democrática de los servicios de inteligencia españoles, dotándoles de mayor transparencia y reforzando la confianza de la ciudadanía en su funcionamiento.

## BIBLIOGRAFÍA

**Aba Catoira, A.**, «El secreto de Estado y los servicios de inteligencia», *Cuadernos Const. De la Cátedra Fadrique Furió Ceriol nº 38/39,* Valencia, 2002.

**Boltaina Bosch, X.**, «Estatuto de personal» en Díaz Fernández, A. M. (dir.): *Conceptos Fundamentales de Inteligencia,* Tirant lo Blanch, 2016.

**Esteban Navarro M. A.**, **Carvalho, A. V.**, «La inteligencia y los activos informacionales» en González Cussac, J. L. (coord.): *Inteligencia,* Tirant lo Blanch, 2012.

**López Temporal, V. M.**, «La investigación policial en los delitos de criminalidad organizada» en González Cussac, J. L., Cuerda Arnau, M. L. (dir.), Fernández Hernández, A. (coord.): *Nuevas amenazadas a la Seguridad Nacional,* Tirant lo Blanch, 2013.

**Lozano Cutanda, B.**, «La desclasificación de los secretos de Estado», *Revista de administración pública*, núm. 146, 1998.

**Garrido Cuenca, N.**, «El episodio judicial de la desclasificación de los papeles del CESID: las sentencias del Tribunal Supremo de 4 de abril de 1997. Paradojas y paralogismos de un conflicto entre la función de gobierno y el derecho a la tutela judicial efectiva», *Revista de Administración Pública*, núm. 143, 1997.

**González López, D.**, «La integración europea en materia de inteligencia: ¿un servicio de inteligencia europeo?», *Studia Humanitatis Journal*, vol. 4, núm. 2, 2024.

**González López, D.**, «La influencia de la inteligencia en el Derecho penal internacional», *ReCrim. Revista de l'Institut Universitari d'Investigació en Criminologia i Ciències Penals de la UV,* núm. 33, 2025.

**Kent, S.**: *Strategic Intelligence for American World Policy*, Princeton University Press, 1949.

**Martínez Galindo, G.**, «Jurisprudencia del Tribunal Constitucional», *Anuario de Derecho Penal y Ciencias Penales,* núm. 63*,* 2010.

**Orts Berenguer, E.**, «Presentación. A propósito de la seguridad» en Orts Berenguer, E (et. al): *Estudios sobre la Ciencia de la Seguridad,* Tirant lo Blanch, 2012.

**Pérez Luño, A.**, *Los derechos fundamentales*, Tecnos, Madrid, 1988.

**Revenga Sánchez, M.**, «El control del Centro Nacional de Inteligencia: una perspectiva comparada», *Revista Española de Derecho Constitucional,* núm. 116*,* 2019.

**Velasco Fernández, F.**: «Ética» en Díaz Fernández, A. M. (dir.): *Conceptos Fundamentales de Inteligencia,* Tirant lo Blanch, 2016.

# ÉTICA, AUTONOMÍA Y OPERATIVIDAD EN INTELIGENCIA: FUNAMBULISMO EN LA ZONA GRIS

**Alejandro López Palma**

*Fundador y Vicepresidente de la Asociación de Jóvenes en Inteligencia, Defensa y Seguridad (INDESEC)*

## 1. Introducción

En las sociedades democráticas contemporáneas, los servicios de inteligencia enfrentan un desafío estructural: operar de manera eficaz frente a amenazas difusas, globalizadas y tecnológicamente avanzadas, sin vulnerar los principios fundamentales del Estado de derecho. Esta cuestión no es nueva, pero se ha intensificado en las últimas décadas debido a la creciente complejidad del entorno estratégico, la presión mediática, el escrutinio judicial y la aceleración tecnológica. La inteligencia ya no se ejerce únicamente en la penumbra de los conflictos armados o la confrontación geopolítica clásica; hoy forma parte de un entramado institucional que requiere, a la vez, eficacia, legalidad, ética y rendición de cuentas. Esta tensión permanente se concentra en lo que muchos autores han denominado la «zona gris» de la inteligencia[1]: un espacio intermedio entre lo legal y lo legítimo, lo secreto y lo transparente, lo necesario y lo moralmente aceptable.

El concepto de «zona gris» no debe entenderse como un vacío normativo ni como una justificación para el abuso, sino como un campo de tensiones inevitables que requieren una gobernanza sofisticada. Lejos de ser un espacio de arbitrariedad, es un entorno en el que se cruzan lógicas diversas: la lógica de la seguridad nacional, la lógica de los derechos humanos, la lógica del interés público, la lógica operativa, y la lógica institucional. Cada decisión en este espacio implica un equilibrio delicado entre fines y medios, entre urgencia y reflexión, entre autonomía táctica y control democrático. Por ello, más que denunciar la existencia de esta zona gris, se trata de comprenderla,

1. Véase Harrington, J., Mccabe, R., *Detect and Understand: Modernizing Intelligence for the Gray Zone*, Center for Strategic and International Studies (CSIS), Washington D. C., 2021.

acotarla, institucionalizarla y gobernarla desde una perspectiva ética e institucional robusta[2].

Este trabajo parte de una premisa central: la eficacia en inteligencia no debe ser concebida como lo opuesto a la legalidad o la ética, sino como una dimensión que sólo se sostiene en el tiempo si está anclada en principios sólidos de legitimidad. Una inteligencia eficaz pero ilegítima, porque viola derechos, actúa fuera del control institucional o erosiona la confianza pública, termina socavando la propia seguridad que pretende proteger. Del mismo modo, una inteligencia excesivamente restringida por controles ineficaces, politizados o burocratizados puede volverse inoperante frente a amenazas reales. El desafío, por tanto, no es elegir entre eficacia o legitimidad, sino construir un modelo que las integre en tensión productiva.

La necesidad de este equilibrio se ha vuelto aún más urgente en el contexto contemporáneo. Por un lado, las amenazas se han sofisticado: terrorismo global descentralizado, ciberespionaje, injerencias extranjeras híbridas, crimen organizado transnacional, proliferación tecnológica, radicalización digital, entre otras. Por otro, los entornos democráticos han evolucionado: existe mayor demanda de transparencia, mayor sensibilidad social ante los abusos del poder, y mayor exigencia judicial respecto a la protección de derechos fundamentales. Esta doble transformación ha colocado a los servicios de inteligencia en un escenario de mayor exposición, menor margen de opacidad y creciente necesidad de legitimación externa e interna.

En este marco, la cuestión de la autonomía operativa cobra especial relevancia. La inteligencia requiere libertad táctica, flexibilidad metodológica y discrecionalidad estratégica para anticipar amenazas, operar en contextos de alta incertidumbre y adaptarse a entornos dinámicos. Sin embargo, esa autonomía no puede ser absoluta. Debe estar enmarcada en un sistema de controles formales e informales que garanticen su compatibilidad con el Estado de derecho. Aquí entra en juego el segundo eje de este trabajo: el control democrático. No se trata solo de fiscalizar resultados o legalidades, sino de establecer una gobernanza de la inteligencia que combine transparencia razonable, supervisión técnica, legitimidad política y ética profesional.

La experiencia internacional ofrece lecciones valiosas al respecto. La creación de comités parlamentarios especializados, la existencia de organismos independientes de auditoría, los mecanismos de revisión judicial, la publicación de informes estratégicos no confidenciales, y la promoción de una cultura de control interno en las propias agencias son ejemplos de herramientas que, combinadas, pueden equilibrar eficacia y rendición de cuentas. No obstante, estos mecanismos presentan desafíos considerables: riesgos de politización, falta de formación técnica de los superviso-

2. Véase Baqués, J., *De la «grey zone» a la zona gris: evolución de un concepto en el marco de los conflictos híbridos*, Instituto Español de Estudios Estratégicos, Madrid, 2019.

res, opacidad normativa, resistencias culturales dentro de los servicios, o incluso la tentación de blindar políticamente ciertas operaciones bajo el pretexto de la seguridad nacional.

Además de la cuestión institucional, también se abordará la dimensión ética de la práctica de inteligencia. La toma de decisiones en contextos grises; donde no hay normas claras, ni soluciones evidentes; exige criterios éticos internalizados, capacidad de deliberación moral, y liderazgo institucional que refuerce estos valores. Sin una ética profesional sólida, las agencias de inteligencia corren el riesgo de degradarse internamente, justificar excesos como necesidad operativa, y perder legitimidad tanto ante sus operadores como ante la sociedad.

Un elemento clave en esta discusión será el análisis de los *Confidence Building Measures* (en adelante CBM) como instrumentos para gestionar la confianza y reducir la incertidumbre en contextos internacionales. Estos mecanismos, originalmente diseñados para evitar conflictos armados accidentales durante la Guerra Fría, han evolucionado hacia formas de cooperación estratégica entre actores con intereses divergentes. Su lógica se ha trasladado también al campo de la inteligencia, donde compartir información, establecer canales de comunicación o acordar protocolos comunes puede contribuir a mitigar tensiones y evitar malentendidos peligrosos. Sin embargo, los CBM también plantean diversas cuestiones: ¿Cuánta información se puede compartir sin comprometer fuentes o capacidades? ¿Cómo evitar que estos mecanismos se conviertan en instrumentos de manipulación estratégica?

Finalmente, el trabajo se centrará en proponer un modelo híbrido de supervisión que articule autonomía operativa con control democrático y ética institucional. Este modelo no será uniforme ni cerrado, sino adaptable a los diferentes contextos nacionales y capaz de integrar aprendizajes históricos, experiencias comparadas y desafíos emergentes como la inteligencia artificial, la privatización del espionaje o la guerra cognitiva. El objetivo no es ofrecer una fórmula definitiva, sino contribuir a una reflexión crítica y propositiva sobre cómo construir una inteligencia eficaz, ética y legítima en el siglo XXI.

## 2. La inteligencia y su evolución ética

La historia de la inteligencia está marcada por una tensión persistente entre eficacia operativa y escrutinio normativo. En sus orígenes, la práctica del espionaje y la obtención secreta de información no requerían justificación ética: se consideraban instrumentos naturales del poder, empleados por monarcas, emperadores y jefes militares para garantizar la supervivencia del Estado y la victoria en el campo de batalla. Heródoto, Sun Tzu o Maquiavelo ya escribían sobre la utilidad de los espías como elementos

imprescindibles del arte de gobernar[3]. En estos marcos, la inteligencia era parte de una razón de Estado absolutista, desligada de consideraciones morales o jurídicas.

Sin embargo, el proceso de institucionalización de la inteligencia, especialmente a lo largo del siglo XX, supuso un cambio cualitativo. La creación de servicios formales de inteligencia en países democráticos, la profesionalización del sector y la consolidación de sistemas constitucionales implicaron la progresiva necesidad de insertar esta actividad en un marco normativo y ético. El paso del espionaje artesanal y patriótico al sistema de inteligencia institucionalizado exigió reglas, procedimientos, controles y, sobre todo, una justificación ante los valores democráticos que se pretendían defender.

El punto de inflexión más importante se produjo tras la Segunda Guerra Mundial. El surgimiento del orden liberal internacional y la creación de organismos multilaterales como Naciones Unidas o el Consejo de Europa impulsaron una nueva sensibilidad sobre los derechos humanos, la transparencia y la responsabilidad estatal. En este nuevo contexto, las actividades secretas del Estado comenzaron a ser observadas con mayor atención crítica. Las democracias ya no podían justificar cualquier exceso en nombre de la seguridad, sin enfrentar tensiones internas y externas.

La Guerra Fría, no obstante, supuso un periodo ambiguo. Aunque se consolidaron estructuras institucionales de inteligencia (como la CIA en Estados Unidos., el MI6 en Reino Unido o el BND en Alemania), también se naturalizaron prácticas de dudosa legalidad: operaciones encubiertas en terceros países, campañas de desinformación, vigilancia masiva de ciudadanos, uso de intermediarios ilegales, e incluso participación indirecta en golpes de Estado. El temor al comunismo, las dinámicas de bloques y la doctrina de la seguridad nacional justificaron, en muchos casos, acciones que hoy serían inaceptables.

En Estados Unidos, la creación de la Comisión *Church* en 1975 marcó un antes y un después. Esta comisión parlamentaria investigó los abusos cometidos por la CIA y el FBI, revelando programas secretos de vigilancia a ciudadanos estadounidenses, intentos de asesinato a líderes extranjeros, experimentos con drogas sobre personas sin su consentimiento, y sabotaje político interno. El informe *Church* no solo supuso una conmoción pública, sino que derivó en reformas legislativas concretas, como la creación del Comité de Inteligencia del Senado y la aprobación de nuevas leyes de supervisión. Por primera vez, se reconocía públicamente que los servicios de inteligencia debían operar dentro de los límites del Estado de derecho y estar sujetos a mecanismos de control democrático.

3. Véase Heródoto, *Historias*, libro VII, cap. 61, trad. Carlos Schrader, Editorial Gredos, Madrid, 1985; Sun Tzu, *El arte de la guerra*, cap. XIII: «El uso de espías», trad. Gabriel García-Noblejas, Editorial Alianza, Madrid, 2014; Maquiavelo, N., *El príncipe*, trad. Miguel Ángel Granada Martínez, Editorial Alianza, Madrid, 2010.

Este proceso tuvo eco en otras democracias. En Alemania, tras los escándalos de vigilancia durante los años 70 y 80, se introdujeron reformas que fortalecieron la supervisión parlamentaria del *Bundesnachrichtendienst* (BND). En Reino Unido, el *Intelligence Services Act* de 1994 legalizó formalmente la existencia del MI6 y estableció mecanismos de rendición de cuentas. Incluso en países con tradiciones de opacidad más arraigadas, como Francia o Italia, se impulsaron medidas para equilibrar la autonomía operativa con ciertas formas de control institucional.

Ahora bien, la legalidad no agota la cuestión ética. Como sostiene OMAND, la ética en inteligencia no puede reducirse al cumplimiento de la ley; exige una reflexión continua sobre los fines y medios empleados, así como una cultura profesional que integre el juicio moral en cada decisión operativa[4]. En otras palabras, no basta con cumplir las normas: hay que deliberar sobre lo correcto, lo justo y lo proporcional.

Esta concepción requiere distinguir entre legalidad, legitimidad y moralidad. Una operación puede ser legal, pero ilegítima desde el punto de vista democrático si, por ejemplo, socava derechos fundamentales o se ejecuta con fines políticos. A su vez, puede ser considerada moralmente reprobable incluso si cumple formalmente con los requisitos legales. Por estos motivos, la ética profesional en inteligencia no debe ser vista como un complemento, sino como un componente central del diseño estratégico.

En este contexto, Velasco Fernández insiste en la necesidad de una «cultura ética robusta» en los servicios, construida sobre formación continua, liderazgo ejemplar, códigos de conducta claros y canales de deliberación interna. A su juicio, «los servicios de inteligencia deben ser regulados por otras instancias del Estado e incluso por instituciones de solvente prestigio (comités éticos) ajenas al Estado. Una institución que se regula a sí misma se condena a cometer excesos o a la corrupción»[5]. Esta advertencia cobra especial relevancia en contextos donde las urgencias operativas, la presión política o la lógica del enemigo pueden llevar a justificar conductas que, con el tiempo, erosionan la propia legitimidad institucional.

Los casos recientes confirman esta tensión. Las revelaciones de Edward Snowden en 2013[6] sobre los programas de vigilancia masiva de la NSA mostraron cómo la tecnología había ampliado la capacidad de los Estados para monitorear a sus ciudadanos sin su conocimiento ni consentimiento. Aunque muchas de estas prácticas eran legalmente autorizadas bajo normativas

4. Véase Omand, D., *Securing the State*, Hurst & Company, Londres, 2010.

5. Velasco Fernández, F., «Ética», en Díaz Fernández, A. M. (dir.): *Conceptos fundamentales de inteligencia*, Tirant lo Blanch, Valencia, 2016, pág. 173.

6. Greenwald, G., Poitras, L., Macaskill, E., «Edward Snowden: the whistleblower behind the NSA surveillance revelations», en *The Guardian*, 9 de junio de 2013. Disponible en: https://www.theguardian.com/world/2013/jun/09/edward-snowden-nsa-whistleblower [consulta: 12 de septiembre de 2025].

como el *Patriot Act*, el escándalo provocó un debate global sobre privacidad, derechos digitales, cooperación entre agencias y confianza ciudadana. De hecho, algunos de los programas revelados fueron posteriormente limitados o declarados inconstitucionales por los tribunales.

Otro caso paradigmático es el uso del software Pegasus, desarrollado por NSO Group, para espiar a periodistas, activistas y opositores políticos en varios países. Aunque los gobiernos implicados alegan razones de seguridad nacional, la opacidad del sistema, la falta de controles judiciales efectivos y el carácter selectivo de los objetivos evidencian una deriva autoritaria en el uso de herramientas de ciberinteligencia. Este tipo de tecnologías permiten a los gobiernos saltarse los controles clásicos (autorizaciones judiciales, supervisión parlamentaria, trazabilidad institucional), lo que convierte la dimensión ética en un eje decisivo de gobernanza.

Todo esto plantea una pregunta clave: ¿Puede existir una ética universal de la inteligencia o cada contexto debe construir su propio marco en función de sus valores, amenazas y estructuras políticas? Si bien es cierto que las culturas de inteligencia difieren según el país, también lo es que existen principios comunes que pueden ser promovidos internacionalmente: proporcionalidad, necesidad, no discriminación, responsabilidad, transparencia limitada, respeto a los derechos fundamentales. Estos principios podrían servir como base para construir un derecho blando de la inteligencia, impulsado por organismos multilaterales y redes profesionales.

En síntesis, la evolución ética de la inteligencia refleja la transformación de las democracias modernas y sus exigencias de control sobre el poder oculto. De una práctica marginal y sin normas, hemos pasado a un sector profesionalizado, regulado y cada vez más sometido al escrutinio público. Pero este camino no está exento de riesgos: los retrocesos autoritarios, el uso indebido de la tecnología, el debilitamiento de los controles o la cultura del secreto pueden hacer retroceder décadas de avances. Por ello, fortalecer la ética en inteligencia no es solo una cuestión normativa, sino un imperativo de legitimidad democrática.

# 3. Confidence Building Measures (CBM): ética y política de la confianza

## 3.1. Origen y fundamentos conceptuales

Los CBM, o medidas de fomento de la confianza, tienen su origen en el contexto bipolar de la Guerra Fría, cuando la amenaza de un conflicto accidental entre superpotencias nucleares era tan real como el enfrentamiento ideológico directo. Ante la posibilidad de que una mala interpretación de maniobras militares o el fallo en una comunicación pudieran desencade-

nar una escalada incontrolable, surgió la necesidad de establecer mecanismos que redujeran la incertidumbre estratégica. Los CBM fueron diseñados como instrumentos pragmáticos para gestionar la desconfianza, más que para eliminarla.

Su consagración institucional se dio en el Acta Final de Helsinki de 1975, firmada en el marco de la Conferencia sobre Seguridad y Cooperación en Europa (CSCE), que más tarde daría lugar a la Organización para la Seguridad y Cooperación en Europa (OSCE). A través de medidas como la notificación previa de ejercicios militares, la invitación de observadores internacionales, el establecimiento de canales de comunicación directa (como el teléfono rojo) y el intercambio de información sobre fuerzas armadas, los CBM introdujeron la transparencia como una herramienta de seguridad, no como una cesión de soberanía. Se trataba, en definitiva, de sustituir la lógica del secreto absoluto por una lógica de transparencia limitada y regulada, suficiente para estabilizar las percepciones mutuas y evitar la escalada accidental.

Los CBM suponen, por tanto, un cambio de paradigma. Este principio ha trascendido su origen militar y se ha extendido a otros ámbitos, como la gestión de fronteras, la cooperación en ciberseguridad, el desarme, la lucha antiterrorista o incluso la gobernanza de la inteligencia. La idea central es que los actores estratégicos pueden cooperar selectivamente, incluso en escenarios de rivalidad, si existen reglas claras, verificación mutua y un nivel mínimo de confianza operativa.

## 3.2. Aplicación al campo de la inteligencia

Aunque los CBM nacieron en el ámbito militar, su adaptación al terreno de la inteligencia ha cobrado fuerza en las últimas décadas. Este proceso no ha sido sencillo, pues la inteligencia es, por naturaleza, una actividad basada en la reserva, la unilateralidad y la protección estricta de fuentes y métodos. No obstante, la globalización de las amenazas y la interdependencia estratégica han empujado a los servicios de inteligencia a establecer formas puntuales de cooperación que, si bien no eliminan el secreto, sí lo regulan y canalizan.

En la actualidad, existen múltiples formatos de CBM aplicados a la inteligencia. Algunos de ellos son bilaterales y basados en acuerdos entre Estados con niveles similares de confianza política. Otros son multilaterales, establecidos en el seno de organizaciones regionales o alianzas estratégicas. Ejemplos relevantes incluyen:

El Club de Berna y el *Counter-Terrorism Group* (CTG): formado por los servicios de inteligencia interior de los países de la UE además de los de Noruega y Suiza, facilita el intercambio de información sensible sobre amenazas yihadistas, movimientos extremistas y riesgos para infraestructuras críticas.

Opera bajo principios de reciprocidad, proporcionalidad y confidencialidad, sin depender de una estructura supranacional.

La iniciativa *Five Eyes*: un acuerdo histórico entre Estados Unidos, Reino Unido, Canadá, Australia y Nueva Zelanda para compartir inteligencia de señales (SIGINT) y otros productos analíticos. Aunque no se autodefine como CBM, actúa como tal al institucionalizar la cooperación y establecer estándares comunes para el manejo de datos clasificados.

Centros regionales de fusión de inteligencia (*fusion centers*): como el *African Union Mechanism for Police Cooperation* (AFRIPOL) o el *ASEAN Counter-Terrorism Centre* (SEARCCT), que permiten a países con capacidades desiguales colaborar mediante protocolos de intercambio seguro de información y asistencia técnica.

OSCE y ciberseguridad: la OSCE ha promovido desde 2013 un conjunto de CBM en el ciberespacio entre sus Estados participantes. Estas medidas buscan mitigar malentendidos en caso de incidentes cibernéticos, mediante la notificación voluntaria de políticas de ciberseguridad, la designación de puntos de contacto nacionales y la implementación de canales de comunicación de emergencia.

## 3.3. Dilemas éticos, políticos y operativos

La implementación de CBM en inteligencia, sin embargo, no está exenta de dilemas profundos. El primero es el riesgo operativo: compartir información implica abrir parcialmente el núcleo de una agencia, exponiendo capacidades técnicas, metodologías o fuentes. Si la confianza depositada se traiciona, el coste puede ser estratégico. En el ámbito de la inteligencia humana (HUMINT), por ejemplo, una filtración puede significar la muerte de una fuente o la ruptura de una red clandestina.

El segundo dilema es la asimetría entre los socios. En muchas iniciativas multilaterales, algunos países tienen capacidades tecnológicas y de análisis muy superiores a otros. Esto puede generar desequilibrios que dificultan la confianza recíproca: ¿Por qué un país con tecnología avanzada compartiría información con otro que no puede protegerla adecuadamente? ¿Cómo se garantiza que los flujos informativos sean equilibrados y no unidireccionales?

El tercer dilema es ético y normativo. Algunos CBM implican compartir información con países que no respetan los estándares internacionales de derechos humanos. ¿Es legítimo transferir inteligencia sobre posibles terroristas si existe el riesgo de que sean detenidos arbitrariamente, torturados o ejecutados? Este dilema fue evidente tras los atentados del 11-S, cuando Estados occidentales colaboraron con regímenes autoritarios en la llamada guerra contra el terror, facilitando detenciones extrajudiciales, vuelos secretos y centros de detención opacos.

Desde una perspectiva ética, como señala WELSH, la cooperación internacional en seguridad debe ser coherente con los valores que pretende defender[7]. Esto implica que los CBM no solo deben ser eficaces, sino también responsables. Requieren garantías institucionales, cláusulas de uso restringido, auditorías independientes y una deliberación permanente sobre su compatibilidad con el Estado de derecho.

Además, está el riesgo de la instrumentalización estratégica. Algunos Estados pueden participar en CBM para ganar legitimidad o desviar críticas, sin intención real de cumplir los compromisos adquiridos. Otros pueden utilizar la información obtenida no para cooperar, sino para debilitar o manipular a sus interlocutores. Por eso, los CBM deben estar acompañados de mecanismos de verificación, sanciones por incumplimiento y marcos multilaterales de revisión.

## 3.4. Potencial de futuro

A pesar de sus limitaciones, los CBM siguen siendo una herramienta con gran potencial para construir una arquitectura de seguridad cooperativa en el siglo XXI. En un mundo cada vez más interconectado, donde las amenazas cruzan fronteras a velocidad digital, y donde ningún Estado puede enfrentar solo los desafíos globales, la cooperación en inteligencia se vuelve indispensable.

El reto es diseñar CBM adaptados a las nuevas realidades: mecanismos ágiles, confiables, éticamente sólidos y técnicamente seguros. Esto implica desarrollar estándares comunes de ciberseguridad, protocolos internacionales de privacidad de datos, mecanismos de coordinación para crisis híbridas, y canales multilaterales de comunicación operativa que funcionen incluso en contextos de tensión política.

El desarrollo de tecnologías de intercambio seguro, como sistemas de intercambio de información segmentado, encriptación de extremo a extremo y blockchain aplicado a trazabilidad documental, puede ayudar a reducir los riesgos operativos. Asimismo, la participación de organismos internacionales y redes académicas puede aportar una capa adicional de legitimidad, evaluación y acompañamiento técnico.

En resumen, los CBM en inteligencia no son la solución definitiva, pero sí un paso imprescindible hacia una gobernanza global de la seguridad que no sacrifique la ética en nombre de la eficacia. Construir confianza entre actores acostumbrados a la desconfianza requiere tiempo, prudencia, creatividad institucional y, sobre todo, voluntad política.

---

7. Véase Welsh, J., *The Return of History: Conflict, Migration, and Geopolitics in the Twenty-First Century*, House of Anansi Press, Toronto, 2016.

# 4. Autonomía operativa vs. control democrático: una tensión estructural

## 4.1. La autonomía como condición funcional de la inteligencia

La actividad de inteligencia, en cualquier sistema político, implica decisiones rápidas, acceso privilegiado a información sensible y capacidad de actuar en entornos de alta incertidumbre. En este contexto, la autonomía operativa es frecuentemente presentada como un requisito funcional para la eficacia[8]. A diferencia de otras instituciones estatales, las agencias de inteligencia operan bajo premisas distintas: el secreto, la anticipación y, en ocasiones, la transgresión temporal de normas comunes para evitar daños mayores.

Esta lógica está particularmente extendida en sistemas presidenciales o de fuerte centralización ejecutiva. En Estados Unidos, por ejemplo, la comunidad de inteligencia cuenta con una flexibilidad táctica derivada del principio de unidad de acción del Ejecutivo, reforzado tras los atentados del 11 de septiembre de 2001. Bajo el marco legal de la *Authorization for Use of Military Force* (AUMF) y la *Patriot Act*, la CIA y la NSA ampliaron sus competencias, incluyendo la conducción de operaciones encubiertas, detenciones extrajudiciales, y programas de vigilancia masiva en colaboración con empresas privadas.

Esta ampliación del margen de acción se fundamentó en la doctrina del daño anticipado (*preemptive harm*), que sostiene que la prevención de amenazas terroristas o cibernéticas justifica la adopción de medidas excepcionales antes de que se materialice el daño. Si bien esta lógica tiene una racionalidad estratégica, plantea también un dilema normativo: cuanto más autónoma es una agencia, menos sujeta está al control democrático y más difícil es asegurar que actúa en conformidad con los valores constitucionales.

## 4.2. Riesgos institucionales y precedentes históricos

Cuando la autonomía se transforma en atribución propia de poder, los servicios de inteligencia pueden actuar como actores autónomos dentro del Estado, generando lo que se ha denominado «Estado dentro del Estado». Este fenómeno ha sido documentado en diversos contextos históricos. La Stasi (Ministerio para la Seguridad del Estado) en la antigua República Democrática Alemana (RDA), la Dirección de Vigilancia del Territorio francesa (DST)

8. Véase Henschke, A., Walsh, P. F., *The Ethics of National Security Intelligence Institutions: Theory and Applications*, Routledge, Londres, 2024.

durante la guerra de Argelia, o el Servicio Secreto del Apartheid en Sudáfrica operaron con una combinación de poder operativo, opacidad y ausencia de control, lo que facilitó violaciones sistemáticas de derechos humanos.

En democracias consolidadas, los riesgos de autonomía sin control también han generado crisis institucionales. El escándalo Irán-Contra en Estados Unidos. mostró como la CIA desvió fondos obtenidos ilegalmente de la venta de armas a Irán para financiar a los contras nicaragüenses, eludiendo la supervisión del Congreso. En Italia, la logia P2 (Propaganda Due) tejió una red clandestina de influencia dentro del aparato de inteligencia militar (SISMI), manipulando decisiones políticas y judiciales durante los llamados años de plomo.

Incluso en sistemas parlamentarios sólidos, la falta de controles eficaces puede llevar a excesos. En el Reino Unido, el programa Tempora permitió la interceptación masiva de comunicaciones por parte del *Government Communications Headquarters* (GCHQ), sin consentimiento ciudadano ni conocimiento público, hasta que fue revelado por Edward Snowden. Aunque legalmente autorizado bajo la *Regulation of Investigatory Powers Act* (RIPA), el programa planteó dudas sobre la proporcionalidad y la compatibilidad con el Convenio Europeo de Derechos Humanos.

## 4.3. Consecuencias políticas y sociales de los abusos

La ausencia de controles efectivos puede derivar en consecuencias devastadoras tanto para la legitimidad del Estado como para el tejido democrático. Cuando se revelan abusos por parte de los servicios de inteligencia, se genera una crisis de confianza ciudadana. La percepción de que las agencias actúan con impunidad erosiona la legitimidad del sistema político y puede alimentar discursos populistas o antisistema.

El caso español ofrece una ilustración reciente. En 2022, el escándalo del uso del software Pegasus para espiar a líderes independentistas catalanes reveló lagunas normativas y debilidades en los controles judiciales sobre el Centro Nacional de Inteligencia (CNI).[9] Aunque el Gobierno justificó legalmente algunas de las interceptaciones, la falta de transparencia y la negativa a desclasificar ciertos documentos provocaron una grave crisis política, debilitando los apoyos parlamentarios del Ejecutivo e internacionalizando la controversia.

9. «El CNI pidió comprar el sistema Pegasus para espiar en el extranjero», en *El País*, 20 de abril de 2022. Disponible en: https://elpais.com/espana/2022-04-20/el-cni-pidio-comprar-el-sistema-pegasus-para-espiar-en-el-extranjero.html [consulta: 12 de septiembre de 2025]; «Así se protegerá el móvil de Pedro Sánchez para evitar otro espionaje como el de 'Pegasus'», en *ABC*, 15 de enero de 2025. Disponible en: https://www.abc.es/espana/protegera-movil-pedro-sanchez-evitar-espionaje-pegasus-20250115150334-nt.html [consulta: 12 de septiembre de 2025].

En democracias en retroceso, los servicios de inteligencia pueden ser utilizados directamente como herramientas de intimidación y represión. El caso de Hungría[10], donde el Servicio de Seguridad Nacional ha sido señalado por colaborar con campañas de vigilancia contra periodistas y activistas críticos con el régimen de Viktor Orbán, muestra cómo la falta de controles judiciales y parlamentarios efectivos facilita la captura autoritaria de las instituciones. Aquí, la inteligencia deja de servir al interés general y pasa a servir al interés particular de quienes ocupan el poder.

## 4.4. Dificultades estructurales del control democrático

El diseño de mecanismos de control enfrenta múltiples obstáculos estructurales. En primer lugar, existe una asimetría informativa inevitable entre las agencias y los órganos de control: quienes deben fiscalizar rara vez tienen acceso completo, tiempo real o capacidad técnica para interpretar adecuadamente la información operativa. Esta brecha genera dependencia de los propios servicios, lo que debilita la autonomía del control.

En segundo lugar, la naturaleza secreta de la actividad de inteligencia dificulta establecer mecanismos clásicos de rendición de cuentas. Las operaciones no pueden revelarse públicamente sin comprometer su eficacia o seguridad. Esto limita el alcance de auditorías externas o del debate parlamentario abierto, exigiendo formatos de supervisión confidencial que, a su vez, dependen fuertemente de la ética personal de los supervisores.

En tercer lugar, hay un problema de voluntad política. Los gobiernos, en muchas ocasiones, utilizan los servicios de inteligencia como herramientas al servicio de su propia agenda, por lo que no tienen incentivos para establecer controles reales. Además, los partidos que hoy están en la oposición y exigen transparencia, mañana podrían estar en el poder y preferir la opacidad. Esta inercia estructural reproduce una cultura de tolerancia institucional al exceso, difícil de revertir sin presión social o reformas estructurales.

## 4.5. Modelos de supervisión: entre el ideal y lo posible

A pesar de estos desafíos, existen ejemplos de buenas prácticas que pueden servir como modelo. El *Intelligence and Security Committee* (ISC) del Parlamento británico es un órgano mixto que combina confidencialidad con

10. «La investigación sobre el 'Irangate' acaba sin desvelar qué sabía Reagan», en *La Vanguardia*, 4 de agosto de 1987. Disponible en: https://hemeroteca-paginas.lavanguardia.com/LVE08/HEM/1987/08/04/LVG19870804-008.pdf [consulta: 12 de septiembre de 2025].

supervisión efectiva. Sus miembros tienen acceso a documentación clasificada, pueden interrogar a altos mandos de la inteligencia y elaboran informes que, si bien se someten a censura de seguridad, son públicos.

En Noruega, el *Control Committee on Intelligence* tiene potestades legales para inspeccionar archivos, entrevistar agentes y emitir recomendaciones con fuerza política, aunque no vinculante. En Canadá, el *National Security and Intelligence Review Agency* (NSIRA) actúa como ente independiente y transversal que coordina la revisión de todas las agencias federales con funciones de inteligencia o seguridad.

En cuanto al poder judicial, su papel es clave, pero también limitado. Los jueces pueden autorizar interceptaciones, registros o detenciones, pero suelen depender de la información que las propias agencias les proveen, lo que puede crear dependencia cognitiva. Además, los recursos judiciales suelen producirse *ex post*, cuando los hechos ya se han consumado, lo que reduce su capacidad preventiva.

## 5. Modelos híbridos de supervisión: hacia un equilibrio sostenible

Frente a la tensión estructural entre eficacia operativa y control democrático en los servicios de inteligencia, una de las soluciones más viables es el desarrollo de modelos híbridos de supervisión. Estos modelos no buscan abolir el secreto ni convertir la inteligencia en una actividad pública, sino diseñar estructuras de control diferenciadas, multilaterales y proporcionales que garanticen tanto la funcionalidad de las operaciones como su sujeción a los principios del Estado de derecho.

En lugar de optar por sistemas monolíticos; excesivamente centralizados o, por el contrario, con control disperso y débil; el enfoque híbrido implica una combinación equilibrada de instancias internas, parlamentarias, judiciales, técnicas e incluso civiles, que actúen de forma articulada y segmentada según el nivel de sensibilidad y el tipo de actividad supervisada.

### 5.1. Supervisión interna especializada

El primer pilar de este modelo debe situarse dentro de las propias agencias. La existencia de unidades internas de supervisión ética y legal, con independencia funcional y acceso irrestricto a las operaciones, constituye una línea de defensa fundamental frente a los abusos y errores. Estas unidades deben estar compuestas por profesionales formados en inteligencia, derecho, derechos humanos y ética pública, y tener capacidad para emitir informes, recomendar cambios y, en casos graves, paralizar operaciones o informar a las autoridades competentes.

Experiencias como el Inspector General de la CIA[11] o las Oficinas de Integridad Institucional en los servicios australianos[12] han demostrado que este tipo de organismos puede actuar eficazmente cuando cuentan con recursos suficientes, respaldo institucional y mandatos claros. Su papel no es solo reactivo, sino también preventivo: identificar patrones de riesgo, alertar sobre desvíos de misión y promover una cultura profesional sensible a los dilemas éticos.

## 5.2. Comisiones parlamentarias reducidas y profesionalizadas

El segundo nivel de supervisión debe estar en manos del poder legislativo. Sin embargo, en lugar de confiar en comisiones parlamentarias amplias o con rotación política frecuente, se propone la creación de comités reducidos, especializados, con acceso a información clasificada y sometidos a obligaciones de confidencialidad. Estos comités pueden estar compuestos por un número limitado de diputados o senadores de distintos grupos, pero con formación específica y asesoramiento técnico independiente.

El modelo británico del *Intelligence and Security Committee* (ISC) es una referencia destacada. Este órgano revisa el funcionamiento del MI5, MI6 y el GCHQ, elabora informes anuales y cuenta con facultades de citación e inspección. Su estructura semipermanente evita que la supervisión sea utilizada con fines partidistas o coyunturales, y su labor ha contribuido a mejorar la percepción pública de la legitimidad de los servicios.

En otros países, como Noruega o Países Bajos, los parlamentos han desarrollado mecanismos similares, con buenos resultados en términos de transparencia controlada y rendición de cuentas adaptada a la sensibilidad del sector[13].

## 5.3. Revisión judicial segmentada y técnica

El poder judicial debe intervenir en el control *ex ante* de ciertas actividades especialmente intrusivas, como la interceptación de comunicaciones, los registros digitales o el uso de tecnologías de vigilancia masiva. No obstante, este control debe adaptarse a la complejidad técnica del entorno actual. Por ello, se propone el establecimiento de jueces especializados en inteligencia, que cuenten con equipos de apoyo técnico, capacidad de acceso a protocolos y facultades de seguimiento.

---

11. CENTRAL INTELLIGENCE AGENCY, *Office of Inspector General*. Disponible en: https://www.cia.gov/about/organization/inspector-general [consulta: 12 de septiembre de 2025].

12. AUSTRALIAN GOVERNMENT, *Inspector-General of Intelligence and Security*. Disponible en: https://www.igis.gov.au/ [consulta: 12 de septiembre de 2025].

13. Véase Peters, B. G., «Institutional Theory in Political Science: The «Norwegian Model» of Parliamentary Oversight», en *Public Administration Review*, 2020.

Este modelo ha comenzado a desarrollarse en algunos sistemas jurídicos. En Francia, la *Commission nationale de contrôle des techniques de renseignement* (CNCTR) actúa como órgano independiente con participación judicial para validar o rechazar solicitudes de técnicas intrusivas. En Canadá, el *Intelligence Commissioner* evalúa determinadas autorizaciones emitidas por el Ejecutivo. Estas estructuras permiten compatibilizar el control judicial con la protección del secreto operativo, sin sobrecargar a los tribunales ordinarios.

## 5.4. Auditorías externas y contralorías técnicas

La supervisión financiera, tecnológica y administrativa puede recaer en organismos externos al circuito político, como tribunales de cuentas, agencias de protección de datos o defensorías del pueblo, siempre que se respete la confidencialidad operativa. Estas instancias permiten verificar el uso adecuado de los recursos, el cumplimiento de normas técnicas o el respeto a los derechos de los afectados por errores o abusos.

En el ámbito europeo, el Supervisor Europeo de Protección de Datos (EDPS) ha intervenido en el control del uso de tecnologías de vigilancia por parte de organismos comunitarios. A nivel nacional, algunas defensorías del pueblo han emitido informes sobre violaciones de derechos en el marco de operaciones de inteligencia, como en los casos del uso de Pegasus en España, donde se solicitó una reforma de la Ley reguladora del CNI para aumentar los controles. Estas auditorías externas, aunque no tienen función operacional directa, constituyen un tercer anillo de legitimidad democrática, al actuar como puente entre la sociedad civil y el aparato estatal secreto.

## 5.5. Publicación de informes desclasificados

Un componente clave del modelo híbrido es la rendición de cuentas a la ciudadanía mediante la publicación periódica de informes no clasificados. Estos documentos no deben revelar fuentes, métodos ni operaciones concretas, pero sí deben ofrecer una panorámica general sobre la estructura, los objetivos estratégicos, el número de operaciones, los errores reconocidos y las reformas institucionales en curso.

En Estados Unidos, la Oficina del Director Nacional de Inteligencia (ODNI) publica un informe anual sobre amenazas y otro sobre transparencia, que incluyen cifras de interceptaciones, autorizaciones judiciales, recursos humanos y recomendaciones internas[14]. En países como Alemania, se publica un

14. Véase Office of the Director of National Intelligence (ODNI), Annual Threat Assessment 2025. Disponible en: https://www.dni.gov/files/ODNI/documents/assessments/ATA-2025-Unclassified-Report.pdf

informe sobre el trabajo del BND que permite al público tener una visión razonablemente informada de la actividad sin comprometer la seguridad.

La publicación de informes tiene un valor simbólico y democrático, pues reduce el aislamiento institucional de la inteligencia y refuerza la percepción de que opera dentro de un marco normativo.

### 5.6. Nombramientos, mandatos y garantías institucionales

Para que este modelo híbrido sea eficaz, es fundamental establecer criterios estrictos de nombramiento, mandatos limitados, rotación periódica y protección frente a represalias para quienes participan en la supervisión. Los miembros de comités de control no deben ser elegidos exclusivamente por el Ejecutivo, sino mediante procedimientos mixtos que garanticen independencia y pluralidad.

Asimismo, deben contemplarse mecanismos de alerta ética (*whistleblowing*[15]), protegidos por ley, que permitan a agentes o funcionarios denunciar abusos o irregularidades sin exponerse a sanciones o despidos. La protección a los denunciantes es una pieza esencial para mantener la integridad del sistema y prevenir desviaciones estructurales[16].

Finalmente, el modelo híbrido debe estar alineado con estándares internacionales, como los del Consejo de Europa, la ONU o las recomendaciones del Parlamento Europeo sobre vigilancia, derechos digitales y transparencia en la seguridad. Esto no implica homogeneizar, sino avanzar hacia mínimos comunes de legitimidad, que permitan a los sistemas nacionales interactuar sin erosionar sus principios.

## 6. Perspectivas futuras y desafíos

La actividad de inteligencia se encuentra en una fase de transformación radical. Los avances tecnológicos, el cambio en la naturaleza de las amenazas, la digitalización de la sociedad y el aumento de la interdependencia glo-

15. Según Hersh, el término alude a la revelación deliberada de información acerca de actividades no triviales que se creen peligrosas, ilegales, inmorales, discriminatorias o que de otra manera incluyen una infracción, generalmente por miembros actuales o pasados de la organización; Como se citó en González López, D., «La Directiva (UE) 2019/1937 relativa a la protección de las personas sobre infracciones del Derecho de la Unión: ¿Qué obligaciones impone a los Estados miembros?», en León Alapont, J. (dir.): *Canales de denuncia en el sector público y privado: whistleblowing y protección del informante (aspectos penales y procesales)*, Colex, 2025, pág. 122.

16. Véase León Alapont, J., *Canales de denuncia e investigaciones internas en el marco del compliance penal corporativo*, Tirant lo Blanch, Valencia, 2023.

bal están redefiniendo las condiciones bajo las cuales operan los servicios de inteligencia. Frente a este nuevo escenario, los desafíos ya no son únicamente operativos o institucionales, sino también epistemológicos, normativos y ético-políticos. Ya no basta con determinar qué se puede hacer, sino qué se debe hacer y bajo qué criterios se justifican las decisiones.

La incorporación de inteligencia artificial (IA) y algoritmos predictivos modifica radicalmente el análisis de datos y la toma de decisiones. Sistemas de *machine learning*, algoritmos de correlación probabilística y procesamiento de lenguaje natural permiten procesar volúmenes masivos de información en tiempo real, desde redes sociales hasta sensores satelitales. Este avance introduce riesgos de opacidad algorítmica, donde ni operadores ni supervisores pueden explicar cómo se generan las predicciones, y de discriminación algorítmica, que reproduce sesgos sociales presentes en los datos. La mitigación de estos riesgos exige auditorías técnicas independientes, marcos éticos claros y comités interdisciplinarios que integren expertos en IA, derechos humanos y seguridad.

El *big data* ha transformado la obtención de inteligencia: información sobre movimientos, comunicaciones y patrones de conducta de millones de personas está disponible a través de fuentes digitales, muchas de ellas generadas voluntariamente. Este fenómeno, conocido como vigilancia por diseño (*surveillance by design*), convierte dispositivos, plataformas y aplicaciones en sensores permanentes. La cooperación entre empresas tecnológicas y agencias de inteligencia difumina los límites entre lo público y lo privado y entre consentimiento y explotación de datos. La ética del consentimiento informado se vuelve limitada y la adquisición de información mediante mercados de datos plantea cuestiones de legalidad y legitimidad. Los retos incluyen establecer límites a la explotación masiva de datos, garantizar el respeto a los derechos fundamentales (*privacy by design*) y regular la retención de información según los principios de necesidad, proporcionalidad y finalidad.

Las amenazas contemporáneas combinan elementos híbridos y zonas grises. Más allá del terrorismo o el espionaje industrial tradicionales, los Estados enfrentan desinformación, ciberataques, presión migratoria instrumentalizada, l*awfare* y sabotaje económico. Estas amenazas carecen a menudo de autoría clara y operan en entornos no convencionales. Rusia, China, Irán y Corea del Norte han perfeccionado operaciones encubiertas digitales mediante *bots*, *trolls* y medios afines, manipulando la opinión pública y erosionando la confianza en instituciones democráticas. Los servicios de inteligencia deben fortalecer la colaboración con instituciones civiles, tecnológicas y de defensa, desarrollando capacidades multidominio. La presión por actuar rápidamente frente a amenazas ambiguas aumenta el riesgo de respuestas desproporcionadas; por ello, son imprescindibles protocolos comunes, mecanismos de verificación internacional, sistemas de alerta temprana cooperativos y marcos normativos que delimiten la acción en ciberespacio y guerra de información.

# 7. Conclusiones

La inteligencia contemporánea transita un territorio tan necesario como complejo: un espacio operativo donde la discreción es una condición funcional, pero la opacidad no puede convertirse en norma; donde la eficacia es un mandato urgente, pero nunca debe erosionar los principios fundamentales de la democracia; donde el secreto protege, pero también puede ocultar abusos si no existen mecanismos adecuados de control. Ese espacio, la llamada zona gris, no es una anomalía del sistema, sino su reflejo cuando alcanza el punto más crítico y revelador.

A lo largo de este trabajo se ha argumentado que la zona gris no puede ser simplemente tolerada ni reprimida, sino gobernada éticamente. Para ello, es imprescindible abandonar visiones maniqueas que contrapongan eficacia y legalidad, operatividad y democracia, seguridad y derechos. En su lugar, debe articularse un enfoque multidimensional que comprenda las lógicas específicas de la inteligencia sin renunciar a someterla a límites estructurales, controles proporcionales y una cultura profesional orientada a la integridad.

Los *Confidence Building Measures* (CBM) han demostrado que incluso en entornos de desconfianza, el intercambio controlado, la transparencia gradual y la verificación recíproca pueden generar entornos de cooperación y prevención. Su valor no reside únicamente en su funcionalidad diplomática, sino en su potencial como arquitectura ética: una forma de construir confianza desde el riesgo compartido y la exposición limitada. El análisis de su evolución y sus dilemas muestra que el equilibrio entre secreto y confianza no solo es deseable, sino posible.

La tensión entre autonomía operativa y control democrático sigue siendo el núcleo más desafiante. Sin libertad táctica, la inteligencia no puede cumplir su misión; sin controles estratégicos, se convierte en un poder sin legitimidad. Por eso, el desarrollo de modelos híbridos de supervisión es una de las tareas centrales para los próximos años. Estos modelos deben ser suficientemente robustos como para detectar abusos, pero también lo bastante flexibles para no paralizar la acción. Su éxito dependerá tanto de su diseño institucional como de la cultura que los sostenga.

Mirando al futuro, los desafíos tecnológicos redefinirán los contornos de la inteligencia. La inteligencia artificial, el big data, la vigilancia algorítmica o las amenazas híbridas ya están transformando no solo cómo se opera, sino qué significa operar con responsabilidad. La velocidad de estos cambios exige una respuesta normativa y ética igualmente innovadora: no basta con adaptar los marcos existentes, es necesario repensarlos desde sus fundamentos.

Frente a estos desafíos, la cooperación internacional, la formación ética de los profesionales y el establecimiento de principios comunes de gobernanza global se perfilan como ejes estratégicos para asegurar una inteligencia alineada con los valores democráticos. La opacidad no debe ser refugio de la

impunidad, sino una herramienta táctica sometida a control. El secreto no puede ser excusa para el abuso, sino un medio legítimo dentro de un marco de legalidad y legitimidad.

En definitiva, la inteligencia no puede escapar a las exigencias de nuestro tiempo. No se trata de desmilitarizarla ni de civilizarla ingenuamente, sino de dotarla de un andamiaje ético-institucional que permita sostener su función estratégica sin renunciar al Estado de derecho. Gobernar la zona gris no es fácil, es, en muchos sentidos, un ejercicio de funambulismo constante, pero es también una condición de posibilidad para la seguridad con dignidad, para la eficacia con justicia, y para una democracia que no renuncie a defenderse sin dejar de serlo.

## BIBLIOGRAFÍA

**Baqués, J.**, *De la «grey zone» a la zona gris: evolución de un concepto en el marco de los conflictos híbridos*, Instituto Español de Estudios Estratégicos, Madrid, 2019.

**Greenwald, G.**, **Poitras, L.**, **Macaskill, E.**, «Edward Snowden: the whistleblower behind the NSA surveillance revelations», en *The Guardian*, 2013.

**González López, D.**, «La Directiva (UE) 2019/1937 relativa a la protección de las personas sobre infracciones del Derecho de la Unión: ¿Qué obligaciones impone a los Estados miembros?», en León Alapont, J. (dir.): *Canales de denuncia en el sector público y privado: whistleblowing y protección del informante (aspectos penales y procesales)*, Colex, 2025.

**Harrington, J.**, **Mccabe, R.**, *Detect and Understand: Modernizing Intelligence for the Gray Zone*, Center for Strategic and International Studies (CSIS), Washington D. C., 2021.

**Heródoto**, *Historias*, libro VII, cap. 61, trad. Carlos Schrader, Editorial Gredos, Madrid, 1985.

**Henschke, A.**, **Walsh, P. F.**, *The Ethics of National Security Intelligence Institutions: Theory and Applications*, Routledge, Londres, 2024.

**León Alapont, J.**, *Canales de denuncia e investigaciones internas en el marco del compliance penal corporativo*, Tirant lo Blanch, Valencia, 2023.

**Maquiavelo, N.**, *El príncipe*, trad. Miguel Ángel Granada Martínez, Editorial Alianza, Madrid, 2010.

**Omand, D.**, *Securing the State*, Hurst & Company, Londres, 2010.

**Peters, B. G.**, «Institutional Theory in Political Science: The «Norwegian Model» of Parliamentary Oversight», en *Public Administration Review*, 2020.

**Sun Tzu**, *El arte de la guerra*, cap. XIII: «El uso de espías», trad. Gabriel García-Noblejas, Editorial Alianza, Madrid, 2014.

**Velasco Fernández, F.**, «Ética», en Díaz Fernández, A. M. (dir.): *Conceptos fundamentales de inteligencia*, Tirant lo Blanch, Valencia, 2016.

**Welsh, J.**, *The Return of History: Conflict, Migration, and Geopolitics in the Twenty-First Century*, House of Anansi Press, Toronto, 2016.

# DE LA LEY DE SECRETOS OFICIALES DE 1968 A LA NUEVA LEY DE INFORMACIÓN CLASIFICADA DE 2025

**César Augusto Giner Alegría**

*Catedrático extraordinario en Ciencias Sociales por la Sociedad de Estudios Internacionales*
*Doctor en abogacía y práctica jurídica*
*Universidad Internacional de Valencia*

**Patrick Salvador Peris**

*Director del Grado en Criminología y Ciencias de la Seguridad*
*Universidad Internacional de Valencia*

## 1. Introducción

En España, el régimen jurídico de los secretos oficiales se ha mantenido durante décadas bajo una norma preconstitucional: la Ley 9/1968, de 5 de abril, sobre Secretos Oficiales, aprobada en plena dictadura franquista y apenas modificada en 1978 antes de la Constitución. Esta ley de 1968 ha sido objeto de crecientes críticas por su obsolescencia y opacidad. Su aplicación ha permitido que numerosos asuntos de interés público permanezcan clasificados indefinidamente, dificultando el escrutinio democrático, la investigación histórica e incluso la persecución de graves violaciones de derechos humanos cometidas en el pasado[1].

La necesidad de una nueva ley se ha vuelto cada vez más importante en el contexto de los compromisos internacionales de España. Como miembro de la Unión Europea y de la OTAN, España debe homologar sus estándares de clasificación de información sensible a los de sus socios. La mayoría de las democracias occidentales disponen de leyes modernas que equilibran la seguridad nacional con el derecho a la información, incluyendo plazos de desclasificación y controles judiciales efectivos. Por ejemplo, países vecinos

1. Alonso de Antonio, Á. L., «La ley de secretos oficiales», en *FORO. Revista de Ciencias Jurídicas y Sociales. Nueva Época*, vol. 18, núm. 1, 2015, pág. 219.

cuentan con sistemas de apertura automática de archivos tras 20, 30 o 50 años según la sensibilidad del material. En España, en cambio, los secretos oficiales podían ser eternos bajo la ley de 1968[2].

En este contexto, el Gobierno español impulsó finalmente en 2022 un Anteproyecto de Ley de Información Clasificada, con el objetivo de sustituir la anticuada ley de 1968 por un marco jurídico acorde al siglo XXI[3]. Tras vicisitudes políticas, el Consejo de ministros aprobó en julio de 2025 el Proyecto de Ley de Información Clasificada y lo remitió a las Cortes Generales para su debate. Se trata de una reforma integral que pretende homologar a España con las democracias más avanzadas en materia de gestión de secretos oficiales, introduciendo categorías de clasificación alineadas con las de la UE/OTAN, plazos máximos de reserva, mecanismos de desclasificación automática y mayores garantías jurídicas.

# 2. Antecedentes normativos

## 2.1. La Ley de Secretos Oficiales de 1968

La Ley 9/1968, de Secretos Oficiales, ha sido el pilar legal y fundamental en materia de información clasificada en España durante más de medio siglo. Promulgada en 1968 por las Cortes de la dictadura franquista, su objeto era regular la información sensible cuyo conocimiento por personas no autorizadas pudiera suponer un riesgo para la seguridad y defensa del Estado. La ley establece el principio general de publicidad de las actuaciones de los órganos del Estado salvo que se declare la materia como «clasificada» por afectar a intereses de seguridad nacional (art. 1). Según su contenido, solo se prevén dos niveles de clasificación —Secreto y Reservado— definidos en el art. 3. Correlativamente, únicamente el Consejo de ministros y el Estado Mayor de la Defensa (Jefe del Estado Mayor) tenían competencia para clasificar o desclasificar información en esos dos niveles máximos.

La Ley de 1968 consta de 14 artículos y venía acompañada de un Reglamento de desarrollo (Decreto 242/1969). Además de los niveles de clasificación mencionados, en la práctica administrativa se introdujeron categorías inferiores de difusión restringida (denominadas «confidencial» y «difusión limitada») para uso interno gubernamental, aunque estos niveles no estaban

2. ESPAÑA, *Ley 9/1968, de 5 de abril, sobre secretos oficiales*, Boletín Oficial del Estado, núm. 84, 6 de abril de 1968. Disponible en: https://www.boe.es/buscar/act.php?id=BOE-A-1968-444

3. GOBIERNO DE ESPAÑA, *Referencia del Consejo de Ministros. Rueda de prensa del Consejo de Ministros, 22 de julio de 2025*, La Moncloa, 22 de julio de 2025. Disponible en: https://www.lamoncloa.gob.es/consejodeministros/resumenes/paginas/2025/220725-rueda-de-prensa-ministros.aspx

previstos expresamente en la ley original. La norma imponía obligaciones de custodiar la información clasificada, establecía quiénes podían acceder según su nivel de autorización, y preveía sanciones —principalmente penales y disciplinarias— para la revelación no autorizada de secretos oficiales[4]. Cabe destacar que la ley excluye expresamente al Congreso de los Diputados y al Senado de las limitaciones de acceso: el propio texto establece que la clasificación no afectará al Parlamento, lo que dio lugar a la creación de la Comisión parlamentaria de Secretos Oficiales para canalizar allí la información secreta que se comparte con los diputados autorizados.

En 1978, en vísperas de la aprobación de la Constitución, se llevó a cabo una reforma de la Ley de Secretos Oficiales mediante la Ley 48/1978, de 7 de octubre, con el fin de adecuarla parcialmente al nuevo contexto democrático. A pesar de aquella actualización limitada en 1978, la Ley de Secretos Oficiales siguió adoleciendo de graves deficiencias desde la perspectiva de una democracia moderna. En particular, la ley no establecía ningún plazo máximo de clasificación: un documento declarado «secreto» o «reservado» podía permanecer indefinidamente oculto, salvo decisión discrecional de desclasificarlo.

## 2.2. Reformas fallidas previas

El inmovilismo normativo en materia de secretos oficiales comenzó a romperse a partir de mediados de la década de 2010, cuando se produjeron los primeros intentos serios de reforma parlamentaria de la ley de 1968. En 2016, el Grupo Vasco (EAJ-PNV) del Congreso de los Diputados presentó una proposición de ley para derogar la vieja norma franquista y establecer plazos de desclasificación automática, iniciativa que contó inicialmente con respaldo mayoritario de la Cámara. Sin embargo, aquel esfuerzo de 2016 no llegó a buen puerto: tras ser admitido a trámite, acabó naufragando por la disolución de las Cortes, ya que los principales partidos (PP y PSOE) prolongaron indefinidamente el plazo de enmiendas en la Mesa del Congreso, bloqueando de facto su avance hasta que la legislatura terminó. Lamentablemente, un patrón similar se repetiría en años subsiguientes.

En 2018-2019, con un nuevo gobierno, volvió a plantearse la necesidad de la reforma, pero la inestabilidad política de aquel periodo impidió concretarla. Posteriormente, en 2020, el PNV nuevamente registró en el Congreso una proposición de ley muy parecida a la anterior (de hecho, era la tercera vez en ocho años que los nacionalistas vascos defendían la reforma). En esta ocasión, la iniciativa también quedó frustrada: aunque todos los grupos salvo PP y Vox eran favorables, la tramitación parlamentaria volvió a dilatarse y

4. García de Paredes Dupuy, A., «¿En qué consiste la Ley de Secretos Oficiales de España?», en *LISA News*, 1 de febrero de 2023. Disponible en: https://www.lisanews.org/inteligencia/en-que-consiste-ley-secretos-oficiales-espana/

quedó interrumpida por la convocatoria adelantada de elecciones generales en 2020, sin que se aprobase la reforma. Cabe señalar que, tanto en 2016 como en 2020, el principal escollo fue la falta de consenso en la Mesa del Congreso para impulsar la proposición de ley —controlada entonces por PP y PSOE—, lo que evidenciaba cierta reticencia bipartidista a abrir los archivos antiguos y limitar la discrecionalidad gubernamental en esta materia[5].

Ante la presión política y social, el propio Gobierno español asumió eventualmente la tarea de redactar una nueva ley. En agosto de 2022, el Consejo de Ministros aprobó un Anteproyecto de Ley de Información Clasificada, esbozando por primera vez la posición oficial del Ejecutivo sobre cómo sustituir la ley de 1968. Aquel anteproyecto de 2022 incorporaba ya las líneas maestras: cuatro niveles de clasificación (en consonancia con los estándares OTAN), plazos concretos para la desclasificación (se mencionaron 25 años prorrogables para secretos, etc., similares a la propuesta del PNV) y mayor control sobre la clasificación. Sin embargo, esa iniciativa se vio truncada por razones de calendario político. No obstante, tras las elecciones de 2023 y la formación de un nuevo Gobierno, el compromiso de renovar la ley de secretos se retomó con fuerza.

## 2.3. Exigencias internacionales y derecho comparado

La actualización de la legislación española de secretos oficiales no ha sido solo una cuestión de política interna, sino también una asignatura pendiente señalada desde instancias internacionales. Diversos organismos y acuerdos multilaterales han instado a España a modernizar su marco normativo, acorde con los estándares democráticos de transparencia y con las necesidades de seguridad compartida en entornos como la OTAN.

En el ámbito de la Unión Europea, el derecho de acceso a la información pública se considera un elemento fundamental del Estado de derecho y de la buena gobernanza. Si bien la UE no impone a los Estados miembros plazos específicos de desclasificación, sí promueve principios de transparencia que resultaban difícilmente compatibles con la Ley 9/1968.

Por su parte, la pertenencia a la OTAN conlleva compromisos estrictos en protección de información clasificada de defensa. La Alianza Atlántica exige que cada Estado miembro disponga de una Autoridad Nacional de Seguridad encargada de salvaguardar los secretos militares compartidos y de aplicar niveles de clasificación equivalentes en todos los países. El Anteproyecto de 2025 crea formalmente la Autoridad Nacional para la Protección de la

5. González, M., «La reforma de la ley franquista de secretos oficiales inicia por tercera vez su tramitación en el Congreso tras dos intentos frustrados», en *El País*, Madrid, 27 de febrero de 2024. Disponible en: https://elpais.com/espana/2024-02-27/la-reforma-de-la-ley-franquista-de-secretos-oficiales-inicia-por-tercera-vez-su-tramitacion-en-el-congreso-tras-dos-intentos-frustrados.html

Información Clasificada y adopta las cuatro categorías de seguridad alineadas con el estándar OTAN (Alto Secreto, Secreto, Confidencial, Restringido).

Desde la perspectiva de los derechos humanos, tanto el Consejo de Europa como las Naciones Unidas han enfatizado que la protección de secretos oficiales debe conciliarse con el derecho a la información y la libertad de expresión. El Tribunal Europeo de Derechos Humanos (TEDH) ha ido construyendo una jurisprudencia relevante: si bien el Convenio Europeo no menciona expresamente un derecho general de acceso a documentos públicos, el TEDH ha reconocido que en ciertas circunstancias ese acceso forma parte del derecho a «recibir informaciones» del Artículo 10 (libertad de expresión).

En el derecho comparado, encontramos modelos diversos que han influido en el debate español. Por ejemplo, en Italia el secreto oficial tiene una duración inicial de 15 años, prorrogable otros 15 como máximo (30 en total), y su declaratoria debe ser motivada por el Primer Ministro ante un comité parlamentario especializado, lo que introduce controles democráticos. En Alemania, la ley fija un plazo general de 30 años para desclasificar los materiales sensibles, aunque tras una reforma en 2017 los servicios de inteligencia pueden solicitar excepciones para no abrir determinados expedientes si consideran que subsisten riesgos. Francia permite la divulgación de documentos de defensa a los 50 años, salvo excepciones muy contadas (por ejemplo, si compromete la seguridad de personas o el secreto de armas de destrucción masiva). Reino Unido, por tradición, aplicaba la llamada «regla de los 30 años» (ahora reducida a 20 años para muchos documentos históricos), aunque conserva la potestad de retener archivos por más tiempo si su difusión perjudicara la seguridad nacional o las relaciones exteriores. Estados Unidos carece de una ley general de secretos oficiales, pero desde 1995 tiene la desclasificación automática a los 25 años para la mayoría de los documentos (con posibles extensiones a 50 o 75 años para información muy sensible, por ejemplo, identidad de agentes o secretos nucleares). Como puede verse, España estaba fuera de estándar: la nueva ley pretende ahora situarla en el rango común (4 a 45 años, prorrogables en ciertos casos), similar a lo que han hecho otras democracias[6].

En el caso particular de Bélgica (que analizaremos más adelante), vale mencionar aquí que hasta fecha reciente tampoco disponía de un procedimiento de desclasificación automático. Bélgica aprobó en 1998 una ley de protección de información confidencial con severas sanciones para filtraciones, pero no previó cómo ni cuándo abrir los documentos. Solo en años recientes, ante críticas, se planteó una reforma: un proyecto de ley (impulsado en 2022 por los partidos ecologistas en el Gobierno belga) propone plazos de 20, 30 o 50 años según el nivel —confidencial, secreto o muy secreto—,

6. RTVE, «De 30 a 75 años: la importancia de la información marca el plazo para revelar secretos oficiales en diversos países», en *RTVE Noticias*, 1 de agosto de 2022. Disponible en: https://www.rtve.es/noticias/20220801/abrir-publico-secretos-oficiales-diversos-paises/2393465.shtml

con un sistema de revisión por la autoridad clasificadora seis meses antes del vencimiento y posible prórroga de 10 en 10 años supervisada por el Parlamento, sin exceder un máximo absoluto de 100 años. Esta referencia belga resulta ilustrativa para España, pues muestra cómo otro país europeo está poniendo límites temporales donde antes no los había, con participación parlamentaria en la prolongación de secretos de Estado.

# 3. El Anteproyecto de Ley de Información Clasificada de 2025

## 3.1. Estructura y principios generales

El anteproyecto se organiza en cuatro títulos que abarcan desde la definición de las categorías de información clasificada hasta el régimen sancionador. En síntesis, el Título I establece las categorías de clasificación y sus definiciones; el Título II regula los órganos competentes y los procedimientos para clasificar, reclasificar y desclasificar; el Título III recoge el régimen jurídico de la información clasificada (acceso, controles, régimen internacional, etc.); y el Título IV contiene el régimen sancionador por infracciones en esta materia. Se incluyen además disposiciones adicionales y finales que tratan aspectos como la adaptación del ordenamiento (por ejemplo, correspondencia entre las nuevas categorías y las anteriores, mandato de adecuación de normas reglamentarias, etc.)[7].

En cuanto a sus principios inspiradores, el texto declara que la clasificación de información tendrá carácter excepcional y deberá ejercerse de forma motivada, conforme a los principios de idoneidad, necesidad y proporcionalidad. Esto significa que solo se podrá clasificar aquello que verdaderamente requiera protección secreta, en la medida estrictamente necesaria para salvaguardar la seguridad o defensa nacional, y proporcionando una justificación escrita de por qué difundir esa información supondría un riesgo. Este énfasis en la motivación y excepcionalidad busca evitar la clasificación abusiva o arbitraria que se denunciaba bajo la ley antigua. El anteproyecto incluso incorpora una prohibición explícita, inédita hasta ahora pues en ningún caso se podrá clasificar información o documentación que afecte a graves violaciones de derechos humanos o a crímenes de lesa humanidad. Con ello se asegura que no se utilice el sello de secreto para encubrir delitos atroces, dando prevalencia al deber de investigar y hacer justicia en esos supuestos.

7. ESPAÑA. CORTES GENERALES. CONGRESO DE LOS DIPUTADOS, *Proyecto de Ley de Información Clasificada*, Boletín Oficial de las Cortes Generales. Serie A. Proyectos de Ley, núm. 65-1, 29 de agosto de 2025.
Disponible en: https://www.congreso.es/public_oficiales/L15/CONG/BOCG/A/BOCG-15-A-65-1.PDF

## 3.2. Categorías de clasificación

El anteproyecto introduce cuatro categorías de información clasificada, que pasan a ser comunes en todo el ámbito estatal. Estas categorías, enumeradas en el artículo 3, son: «Alto Secreto», «Secreto», «Confidencial» y «Restringido». Se trata, ni más ni menos, de los niveles equivalentes a los empleados en la mayoría de los países de la OTAN y la UE, con lo cual España adopta la misma terminología y gradación de protección. Cada categoría se define según la gravedad del daño que la revelación no autorizada de esa información podría causar a la seguridad o defensa nacionales:

a) Alto Secreto: corresponde a la información que requiere el grado más alto de protección, ya que su divulgación sin autorización o uso indebido «podría suponer una amenaza o un perjuicio extremadamente grave para la seguridad nacional o la defensa». En esta categoría se incluirían, por ejemplo, planes militares estratégicos, identidades de agentes encubiertos, inteligencia crítica, o negociaciones diplomáticas de máximo secreto cuya exposición pondría en peligro inmediato la integridad del Estado. El anteproyecto detalla ámbitos en los que cabe esta clasificación excepcional, tales como la soberanía e integridad territorial, la seguridad del Estado y el orden constitucional, la protección efectiva de las fuerzas armadas españolas o aliadas, la seguridad de operaciones de inteligencia, las relaciones exteriores en contextos sensibles, o determinados intereses económicos estratégicos de repercusión en la seguridad nacional.

b) Secreto: se aplica a información que necesita un alto grado de protección, porque su revelación no autorizada podría ocasionar un daño grave a la seguridad o defensa nacional, si bien no tan extremo como en la categoría anterior. Es decir, los secretos serían materiales muy sensibles cuya difusión causaría perjuicios serios (por ejemplo, planes militares tácticos, informes de inteligencia importantes, negociaciones diplomáticas delicadas, etc.), pero que no alcanzan el nivel crítico de alto secreto. La diferencia entre Secreto y Alto Secreto radica principalmente en la intensidad del posible daño (grave vs. extremadamente grave) y, consecuentemente, en los plazos de reserva establecidos (como veremos, 35 años vs. 45 años respectivamente, antes de la desclasificación automática).

c) Confidencial: esta categoría se destina a información cuya divulgación no autorizada podría causar algún perjuicio o amenaza a la seguridad o intereses del Estado, pero de manera más limitada o moderada. Sería información sensible que justifica protección, pero que no llegaría a provocar daños graves en caso de filtración. Por ejemplo, podrían etiquetarse como confidenciales ciertos planes gubernamentales de seguridad ciudadana, informes internos de organismos de seguridad, evaluaciones de riesgos, etc., cuya revelación sería per-

judicial pero manejable. En la escala de riesgo, Confidencial equivale a un nivel medio de daño potencial.

d) Restringido: la categoría más baja, que abarca información cuya revelación no autorizada causaría un perjuicio leve o algún tipo de amenaza limitada para la seguridad nacional. Aquí encajarían documentos de carácter reservado, pero de menor sensibilidad —por ejemplo, comunicados internos, especificaciones técnicas o datos operativos de bajo impacto— que conviene proteger para evitar inconvenientes o vulnerabilidades, aunque su filtración no comprometería seriamente la defensa o seguridad del Estado. La ley subraya que para lo Restringido no se justifica un periodo prolongado de secreto: de hecho, como veremos, es la única categoría cuya información se desclasificará en plazos muy breves (4-5 años) sin posibilidad alguna de prórroga.

La introducción de cuatro niveles supone una novedad importante respecto al sistema antiguo de solo dos niveles (secreto/reservado). En realidad, el Estado español ya manejaba internamente niveles de «confidencial» y «difusión limitada» (similar a restringido) para cierto flujo de información, pero carecían de reconocimiento legal pleno. Ahora pasan a estar formalmente definidos en la ley, lo que aporta claridad. Cada categoría conlleva un nivel de protección distinto, adecuando las medidas de seguridad al riesgo: así, Alto Secreto implica los protocolos de custodia más estrictos, autorizaciones de acceso muy restringidas, registros especiales, etc., mientras que Restringido puede manejarse con medidas de seguridad básicas. Esta proporcionalidad en la protección está alineada con la práctica internacional e impide la tendencia a «sobreclasificar» información de poca sensibilidad con niveles demasiado altos. De hecho, el anteproyecto explícitamente prohíbe marcar información con un nivel superior al que objetivamente requiera; clasificar por encima (*overclassification*) sería contrario al principio de proporcionalidad.

## 3.3. Plazos de desclasificación

Uno de los aspectos más trascendentales —y más esperados— de la nueva ley es la introducción de plazos máximos de vigencia de la clasificación. Por primera vez en la historia española, se consagra el principio de desclasificación automática transcurrido cierto tiempo para cada nivel de secreto. Los plazos previstos en el anteproyecto son los siguientes:

a) Alto Secreto: 45 años, prorrogables excepcionalmente por hasta 15 años adicionales. Es decir, la regla general será que toda información altamente secreta abra al público a los 45 años de su clasificación, salvo que al acercarse ese vencimiento el Gobierno justifique una prórroga (caso por caso) por motivos de seguridad nacional toda-

vía vigentes, pudiendo prolongarla hasta un máximo de 60 años en total. Solo se permite una prórroga, según se desprende del límite de 15 años. Llegado el año 60, en principio, incluso los documentos más sensibles deberían liberarse definitivamente (no se contempla en la ley ninguna categoría permanente más allá de ese horizonte).

b) Secreto: 35 años, prorrogables excepcionalmente por hasta 10 años más. En este nivel, el plazo base es menor —35 años— dada la menor gravedad del daño en caso de revelación. Se prevé igualmente la posibilidad de una prórroga única de hasta una década, lo que significa que como mucho un secreto podría permanecer clasificado 45 años en total. Cabe notar que 45 años era justamente el plazo propuesto en su día por el PNV para secretos (25+10 años) y coincide con lo que otros países manejan para niveles altos.

c) Confidencial: 7 años mínimo y 9 años máximo, sin prórroga alguna. Esta formulación de «entre 7 y 9 años» en la nota de prensa oficial sugiere que la desclasificación de lo confidencial se producirá al término del año natural en que se cumpla aproximadamente el octavo aniversario (por ejemplo, si se clasifica en marzo de 2025, podría desclasificarse automáticamente el 31 de diciembre de 2032, lo cual en la práctica son entre 7 y 8 años y pico; de ahí el rango 7-9). En cualquier caso, es claro que antes de 10 años toda información confidencial debe quedar accesible, y la ley no permite extender ese plazo. Esto es importante: a diferencia de alto secreto o secreto, donde el Gobierno puede apelar a circunstancias excepcionales para retener un tiempo más los documentos, en confidencial y restringido no hay esa facultad. Pasado el plazo, se abren sí o sí.

d) Restringido: 4 años mínimo y 5 años máximo, sin prórroga. De forma análoga al caso anterior, esto implica que aproximadamente a los 5 años (o antes) expirará la clasificación de información restringida. Son plazos muy breves, acordes con la naturaleza menos sensible de esta categoría. Por ejemplo, un informe restringido emitido en 2025 sería público como tarde el 31 de diciembre de 2030[8].

## 3.4. Autoridades competentes

La nueva ley redefine qué órganos y autoridades del Estado tendrán la competencia para clasificar, reclasificar y desclasificar información en cada nivel, estableciendo un esquema más centralizado para los niveles superiores y delegando con cautela en niveles inferiores. Esto conlleva también la creación de un órgano especializado —la mencionada Autoridad Nacional— para coordinar la materia.

8. Gobierno de España, *op. cit.*, págs. 1-4.

Según el anteproyecto, la potestad de clasificar y desclasificar en categoría «Alto Secreto» o «Secreto» corresponderá única y exclusivamente al Consejo de Ministros, a propuesta del Presidente del Gobierno o del ministro competente en el asunto.

Para los niveles inferiores, «Confidencial» o «Restringido», la ley habilita a «un número tasado y reducido de autoridades» para que puedan clasificar y desclasificar. Dichas autoridades son enumeradas en el texto y básicamente incluyen: el Presidente del Gobierno, los Vicepresidentes, todos los Ministros, el Secretario de Estado de Seguridad (del Ministerio del Interior), la Secretaria General de Instituciones Penitenciarias, la Directora del Centro Nacional de Inteligencia (CNI), el Jefe del Estado Mayor de la Defensa (JEMAD), y los Jefes de Estado Mayor de cada uno de los Ejércitos (Tierra, Aire/Espacio, Armada). Esta lista comprende, como se ve, a la cúpula del poder ejecutivo civil y militar.

De esta forma, un documento Confidencial o Restringido podrá ser declarado como tal por, digamos, el Ministro de Defensa en su ámbito o por la Directora del CNI en el suyo, etc., sin necesidad de elevar al Consejo de Ministros. Pero si ese mismo documento requiriese ser Secreto, ya tendría que pasar por Consejo. Esto genera un sistema escalonado de autorizaciones alineado con la sensibilidad: a mayor nivel, más alto el órgano que decide.

Adicionalmente, el anteproyecto crea la figura de la Autoridad Nacional para la Protección de la Información Clasificada (ANPIC), que actuará como ente coordinador y supervisor en esta materia. Según el artículo 6, la Autoridad Nacional se incardina en el Ministerio de la Presidencia, Relaciones con las Cortes y Memoria Democrática (actual departamento de la Presidencia del Gobierno).

El Centro Nacional de Inteligencia (CNI), aunque no es «la autoridad nacional» en sentido formal, mantiene un papel crucial: su Directora puede clasificar documentación confidencial o restringida dentro del ámbito de inteligencia, como hemos visto, y es previsible que el CNI aporte los medios y experticia para buena parte de la protección de secretos. Además, en tanto que principal órgano de inteligencia del Estado, el CNI seguirá siendo usuario y custodio de un gran volumen de información secreta, por lo que la ley también le atañe directamente. Es reseñable que en el debate político algunos grupos pidieron reformar también la ley de control judicial del CNI en paralelo (Junts per Catalunya lo reclamó), pero eso es otra cuestión. En el texto de información clasificada, al CNI se le menciona sobre todo como uno de los actores autorizados a clasificar niveles medios, y deberá obviamente coordinarse con la Autoridad Nacional para aplicar las directrices comunes de seguridad de la información.

El Consejo de Ministros sigue siendo el órgano supremo en esta materia. Cada clasificación de nivel alto la aprobará mediante acuerdo. Asimismo, se prevé que el Consejo de Ministros apruebe reglamentos y directivas de seguridad para desarrollar la ley; por ejemplo, habrá que dictar un Reglamento

de la Ley de Información Clasificada que detalle procedimientos, formatos de marcado, medidas de almacenamiento, etc., probablemente a propuesta de la nueva Autoridad Nacional o del Ministerio de Presidencia. El hecho de que Presidencia asuma la cartera de esta Autoridad indica que el Gobierno le otorga una importancia transversal y que quiere centralizar la política de clasificaciones en Moncloa, más que en cada ministerio por su lado.

En relación con las Comunidades Autónomas, la ley reconoce que algunas CCAA pueden tener materias de seguridad asumidas estatutariamente (por ejemplo, policía autonómica) y por tanto manejar información clasificada. Para ello, se prevé la posibilidad de delegar ciertas funciones en autoridades autonómicas, siempre informando a la Autoridad Nacional. Es una previsión de coordinación para que la protección sea homogénea en todo el Estado, respetando a la vez competencias regionales.

## 3.5. Procedimiento de clasificación y desclasificación

El anteproyecto dedica varios capítulos a establecer los procedimientos garantistas que deberán seguirse tanto para clasificar información como para desclasificarla o cambiar su nivel (reclasificar). El objetivo es dotar de transparencia y control a lo que antes era un proceso opaco y discrecional.

En líneas generales, cuando una autoridad competente considere que cierta información debe ser clasificada, deberá emitir un acto administrativo expreso de clasificación, indicando la categoría asignada, los motivos concretos (fundamentados en las amenazas o perjuicios que divulgarla supondría) y el plazo de vigencia de la clasificación conforme a la ley. Es decir, desde el inicio quedará fijada la «fecha de caducidad» (por ejemplo: «clasificado Secreto hasta el 31/12/2058» si son 35 años) y, en su caso, las condiciones para prórroga si fuera Alto Secreto/Secreto. Este acto se inscribirá en un Registro de diligencias de clasificación llevado por la Autoridad Nacional, para asegurarse de que cada documento clasificado esté inventariado. De hecho, la ley crea registros específicos: de diligencias de clasificación, de directivas de seguridad, etc., centralizados por la Autoridad Nacional. Esto supone un avance en la trazabilidad, evitando que existan «secretos olvidados»[9].

El procedimiento de clasificación puede incluir una figura de clasificación provisional en situaciones de urgencia: por ejemplo, si surge un asunto repentino que requiere secreto inmediato, una autoridad autorizada podría marcarlo como confidencial provisional y luego solicitar la aprobación formal. El anteproyecto prevé que cualquier clasificación (especialmente las de Alto Secreto o Secreto) hechas provisionalmente deben ser ratificadas o revocadas por el Consejo de Ministros en breve plazo. Esto evita que algo quede clasificado de facto sin pasar por el filtro colegiado cuando así se exige.

9. ESPAÑA. CORTES GENERALES. CONGRESO DE LOS DIPUTADOS, *op. cit.*, págs. 5-6.

En cuanto a la desclasificación, se podrá producir de tres maneras: automática por vencimiento de plazo (como ya explicamos, ocurre ipso iure al llegar la fecha); anticipada por decisión de la autoridad competente (si esta considera que ya no es necesario el secreto, puede emitir un acto desclasificando antes del plazo, lo cual se notificará también al Registro); o por orden jurisdiccional en caso de estimarse un recurso. La ley detalla el marco aplicable a la desclasificación y reclasificación en un capítulo específico, subrayando que la desclasificación es una de las novedades que introduce la ley como procedimiento normalizado (antes ni se contemplaba).

Una innovación importante es la posibilidad de reclasificar, es decir, cambiar de nivel de clasificación (tanto al alza como a la baja) antes de la desclasificación final. Por ejemplo, si inicialmente se marcó algo como Alto Secreto, pero tras unos años el riesgo disminuye, el Gobierno podría reclasificarlo a Secreto o Confidencial, lo que implicaría también acortar su plazo de reserva. O viceversa, si se subestima algo y se marcó como confidencial pero luego se ve que es muy delicado, se podría elevar a Secreto, con aprobación correspondiente. La reclasificación, obviamente, debe estar sujeta a motivación y a la competencia del órgano según la categoría a la que se mueve la información. La ley previene posibles abusos: reclasificar para evadir la caducidad (por ejemplo, pasar de Secreto a Alto Secreto solo para obtener 10 años más) no debería ser permitido salvo que realmente se justifique un cambio en la valoración del daño.

## 3.6. Régimen sancionador

La última pieza del anteproyecto es el régimen sancionador administrativo, destinado a penar las conductas contrarias a la ley en materia de información clasificada. Aquí es donde la nueva norma ha generado polémica, pues introduce multas muy elevadas para ciertas infracciones, lo que algunos sectores han criticado por su posible efecto disuasorio sobre la prensa y la sociedad civil.

El Título IV del anteproyecto tipifica una serie de infracciones administrativas, clasificándolas en muy graves, graves y leves, con sanciones pecuniarias máximas de 2,5 millones, 800.000 euros y 30.000 euros respectivamente. En particular, se consideran infracciones muy graves aquellas conductas que supongan una amenaza relevante para la defensa o la seguridad nacional, normalmente vinculadas a información de nivel Alto Secreto o Secreto.

Las infracciones graves comprenden conductas similares pero referidas a información Confidencial. Por ejemplo, difundir sin permiso un documento confidencial se considera infracción grave, sancionable con multa de 30.001 hasta 800.000 euros.

Las infracciones leves se refieren sobre todo a información Restringida o a incumplimientos menores de procedimientos. Por ejemplo, difundir indebi-

damente un documento Restringido se sancionaría como leve, con multa de hasta 30.000 euros. Igualmente, supongo que dejar sin vigilancia un documento de bajo nivel, o no rotular correctamente un clasificado, etc., podrían considerarse leves si no ocasionan mayor peligro.

El anteproyecto detalla unas diez causas que configuran las infracciones más graves, lo cual indica un esfuerzo por describir las conductas típicas a sancionar: desde la filtración intencional a la negligencia grave en custodia. Se complementa así la normativa penal vigente: hay que recordar que, al día de hoy, la revelación de secretos oficiales ya es delito en ciertos supuestos (por ejemplo, para autoridades o funcionarios que revelen secretos que afecten a la seguridad del Estado, el Código Penal prevé penas de prisión de 1 a 4 años; y en el Código Penal Militar, para militares que revelen secretos de servicio, hay penas más altas)

La razón es cubrir supuestos en que intervengan personas no sujetas al código penal (por ejemplo, periodistas o ciudadanos que reciban información clasificada pero no les sea aplicable delito porque no tenían deber de secreto oficial) o conductas de riesgo que no lleguen a materializar delito. Así, la ley impondrá multas a personas físicas o jurídicas (incluso medios de comunicación) que difundan secretos oficiales sin autorización. Esto es exactamente lo que ha encendido alarmas en el gremio periodístico: ¿se multará a periodistas o medios por publicar filtraciones de alto secreto? En teoría, sí[10].

# 4. Transparencia y acceso a la información

## 4.1. Derecho de acceso de periodistas, historiadores y ciudadanos

En una democracia, el acceso a la información pública es tanto un derecho de los ciudadanos como una herramienta para el control del poder. El Anteproyecto de Ley de Información Clasificada (2025) viene a integrar por fin la política de secretos oficiales con la política de transparencia, estableciendo cauces para que, llegado el momento, la información actualmente secreta pueda ponerse a disposición del público[11]. Como ya hemos descrito, la pieza clave es la introducción de plazos de desclasificación automática, que garantizan que transcurrido el tiempo previsto la información pase al dominio público. Esto, por sí solo, supone un enorme avance para investigadores,

10. EL CONFIDENCIAL, «El Consejo de Estado pide revisar la ley de información clasificada y alerta sobre las sanciones a periodistas», en *El Confidencial*, 15 de julio de 2025. Disponible en: https://www.elconfidencial.com/espana/2025-07-15/consejo-estado-informacion-clasificada-sanciones-periodistas_4172252/

11. Malalana Ureña, A.; Moreno Pérez, L., «La Ley de Secretos Oficiales, lastre para la investigación histórica», en *Ayer*, núm. 110, 2018, pág. 333.

periodistas e interesados: se podrá acceder legalmente a archivos históricos sin necesidad de autorizaciones especiales una vez cumplido el plazo[12].

Ahora bien, la ley no se limita a esperar la caducidad; también contempla el acceso antes del vencimiento en ciertos supuestos. En primer lugar, habilita la posibilidad de que cualquier persona con interés personal o profesional solicite la desclasificación de un documento una vez haya vencido su plazo o incluso antes, si entiende que ya no se justifica el secreto.

El anteproyecto utiliza el concepto de «interés legítimo» para delimitar quién puede acceder o solicitar acceso a información clasificada antes de su divulgación general. No se trata de un acceso libre a cualquiera en cualquier momento (porque eso vaciaría la protección), sino de reconocer que ciertos actores tienen un interés cualificado en conocer información, ya sea para el ejercicio de un derecho o para cumplir una función social relevante.

## 4.2. Límites: seguridad nacional vs. derecho a la información

Pese a los avances mencionados, la nueva ley deja en claro que el límite fundamental al acceso a la información sigue siendo la seguridad nacional y la defensa del Estado. En todo momento, la prevalencia o no de uno u otro derecho se analizará bajo el principio de proporcionalidad: se debe ponderar cuánto dañaría revelar cierta información a la seguridad frente al valor informativo o interés público de su difusión[13].

La legislación propuesta formula varios candados para asegurar que la divulgación de información clasificada no comprometa intereses esenciales del país. En primer lugar, mientras la información se encuentre dentro de su plazo de clasificación, rige una presunción de reserva: se entiende que su publicidad es perjudicial y por tanto se mantiene secreta. Solo si concurren circunstancias extraordinarias (por ejemplo, que la razón del secreto haya desaparecido anticipadamente) se consideraría levantarla antes. Esto significa que el derecho a la información cede temporalmente ante la seguridad nacional durante ese lapso.

El derecho a la información de la ciudadanía se verá beneficiado por la mayor cantidad de documentos que saldrán a la luz, pero es cierto que la nueva ley sigue poniendo la vara bastante alta en plazos (45-60 años para altos secretos). Algunos analistas consideran que esos plazos son demasiado largos y que se podría haber optado por 30 años como muchos países.

12. Rey Martínez, F., «Derecho de acceso a la información y secretos oficiales en el ordenamiento español», en *Cuadernos Manuel Giménez Abad*, núm. 5, 2013, pág. 192.

13. Díaz Matey, G., Cremades Guisado, Á., «Los secretos oficiales en España: un dilema entre transparencia y seguridad nacional», en *Gladius et Scientia. Revista de Seguridad del CESEG*, núm. 1, 2019.

Sin embargo, la seguridad nacional seguirá primando como límite al acceso cuando esté en juego una amenaza vigente y seria.

### 4.3. Excepciones: violaciones graves de derechos humanos y crímenes de lesa humanidad

Un aspecto destacable y éticamente relevante del anteproyecto es la cláusula de excepción humanitaria: prohíbe clasificar información que verse sobre graves violaciones de derechos humanos o crímenes de lesa humanidad. Esta disposición, que en el texto aparece como una novedad subrayada por el ministro de Presidencia, responde a una vieja reclamación de organismos de derechos humanos y de memoria histórica, así como a estándares internacionales. En la práctica, significa que el Estado no podrá ampararse en secreto oficial para negar información relativa, por ejemplo, a torturas, genocidio, terrorismo de Estado, desapariciones forzadas, etc. Si existieran archivos o informes que documenten violaciones graves de derechos fundamentales, estos no pueden ser declarados secretos bajo la nueva ley. Y si actualmente algunos lo estuvieran, se debería proceder a su desclasificación inmediata, puesto que su propia naturaleza los excluye del ámbito de protección.

Concretamente, esto tiene enorme repercusión en materia de Memoria Histórica en España. Durante la dictadura franquista y la transición hubo numerosos actos constitutivos de violaciones graves de derechos (ejecuciones extrajudiciales, torturas, desapariciones, etc.). Muchos expedientes relacionados con esos hechos han permanecido inaccesibles, con la Ley de Secretos de 1968 sirviendo de excusa para no abrir archivos de policía, Guardia Civil, ejército o inteligencia de la época. La nueva ley, en conjunción con la reciente Ley de Memoria Democrática 20/2022[14], viene a quitar ese candado.

La protección de derechos humanos se erige en límite absoluto al secreto oficial en la nueva normativa. Se establece que la seguridad nacional nunca podrá esgrimirse para ocultar violaciones graves de derechos o crímenes contra la humanidad.

## 5. Perspectiva comparada: Colombia y Bélgica

En el caso de Colombia, su aproximación a los secretos oficiales ha sido peculiar debido al largo conflicto interno y los procesos de paz. Colombia cuenta desde 2014 con una Ley de Transparencia (Ley 1712/2014) que reconoce el derecho de acceso a la información pública, pero también contempla excepciones por información clasificada o reservada. A diferencia de España,

14. ESPAÑA, *Ley 20/2022, de 19 de octubre, de Memoria Democrática*, Boletín Oficial del Estado, núm. 252, 20 de octubre de 2022, p. 144186-144257. Disponible en: https://www.boe.es/buscar/act.php?id=BOE-A-2022-17099

Colombia no tiene una ley específica de Secretos Oficiales con niveles tipo OTAN; en su lugar, la clasificación de información se rige por normas dispersas[15]. La Constitución colombiana de 1991[16], en su artículo 74 consagra el derecho a acceder a documentos públicos salvo ley en contrario, y la Ley 1712/2014[17] desarrolló esto estableciendo que toda entidad pública debe mantener un Índice actualizado de Información Clasificada y Reservada, indicando qué documentos ha marcado como tales y la motivación y norma que lo avala. Es decir, hay un esfuerzo de transparencia incluso sobre lo reservado: se publica un índice que informa al ciudadano de la existencia de esos secretos[18].

En la práctica colombiana, los términos «clasificada» y «reservada» se usan: clasificada suele referir a información que por normas de seguridad nacional se protege (por ejemplo, inteligencia, contrainteligencia, defensa), y reservada a información cuya publicidad afectaría derechos de terceros o la seguridad (por ejemplo, investigaciones en curso). Una ley crucial es la Ley Estatutaria 1621 de 2013 sobre inteligencia y contrainteligencia, que regula esas actividades y declara secretos los documentos de inteligencia por un período de 40 años, prorrogables por 5 años adicionales indefinidamente (lo cual ha sido criticado). De hecho, la Corte Constitucional colombiana, en sentencia de 2019, pidió delimitar mejor esos plazos porque dejaba posibilidad de secreto indefinido. Hay iniciativas para reformar la Ley 1621 y reducir esos tiempos, en línea con la transparencia del acuerdo de paz, que exige abrir archivos de la guerra para la Comisión de la Verdad y la Jurisdicción Especial de Paz.

Una innovación importante en Colombia fue, tras el acuerdo de paz de 2016, la orden de desclasificar archivos de inteligencia anteriores a 1991 para esclarecer violaciones de derechos humanos durante el conflicto. Esto es similar a nuestra cláusula: se reconoció que la verdad histórica primaba. Sin embargo, su implementación ha sido lenta. Organizaciones como *Dejusticia* demandan desclasificar los archivos de inteligencia previos a 1991, demostrando que, en Colombia, como aquí, la sociedad civil presiona por mayor apertura.

En cuanto a periodistas, Colombia en 2021 aprobó una Ley de Protección de Fuente y Periodistas, pero aún hay tensión: la filtración de documentos está

15. ARCHIVO GENERAL DE LA NACIÓN (COLOMBIA): *Guía para la calificación de la información (GIT-G-01)*, Bogotá, 2014. Disponible en: https://www.archivogeneral.gov.co/sites/default/files/Estructura_Web/3_Transparencia/3.3%20Procesos%20y%20Procedimientos/GIT-G-01_GUIA_PARA_LA_CALIFICACIÓN_DE_LA_INFORMACIÓN_AGN.pdf

16. COLOMBIA, *Constitución Política de Colombia*, Diario Oficial de Colombia, núm. 44.109, 4 de julio de 1991. Disponible en: https://www.constitucioncolombia.com/

17. COLOMBIA, *Ley 1712 de 2014, de 6 de marzo, por la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones*, Diario Oficial de Colombia, 6 de marzo de 2014. Disponible en: https://www.suin-juriscol.gov.co/viewDocument.asp?ruta=Leyes/1687091

18. MÁS INFORMACIÓN, MÁS DERECHOS, «¿Cuáles documentos son secretos en Colombia?», en *Más información, más derechos*, 31 de julio de 2014. Disponible en: https://masinformacionmasderechos.co/2014/07/31/cuales-documentos-son-secretos-en-colombia-2/

penada si se considera que violas secretos de Estado, aunque los casos han sido pocos. Cabe destacar que en el *ranking* de *Right to Information* (RTI) 2022, la ley de transparencia colombiana obtuvo 92/150 puntos, mejor que la española (89/150), por aspectos como la existencia de ese índice de clasificados[19].

Con respecto a Bélgica ofrece un caso interesante porque, como España hasta ahora, fue acusada de rezagada en materia de secretos oficiales. Históricamente, Bélgica no contaba con plazos de desclasificación automática. Tenía la Ley de 11 de diciembre de 1998 sobre clasificación y seguridad (adaptada al introducir le marco OTAN y UE tras la Guerra Fría), que estableció niveles (*Très Secret, Secret, Confidentiel*) y penas por divulgar secretos, pero no previó mecanismos de desclasificación temporal. Así, los documentos quedaban clasificados hasta que una autoridad decidiera lo contrario, cosa que raramente ocurría. Este vacío fue señalado por la prensa y políticos belgas como problemático.

Para contextualizar, en Bélgica el gobierno designa la clasificación, pero no existía un «caducador» temporal. Por ejemplo, expedientes de la época de la Guerra de Ruanda con implicación belga han permanecido cerrados, generando controversias y peticiones de abrirlos para la verdad histórica. Bajo la presión de ecologistas (*Ecolo/Groen*) y archivistas, en 2020-2021 se impulsó un proyecto de ley de desclasificación. En efecto, en 2022 se introdujo en el Parlamento belga una reforma apoyada por la coalición de gobierno (llamada Vivaldi) que propone: un documento *Confidentiel* se abra a los 20 años, *Secret* a los 30, *Très Secret* a los 50 años. Con posibilidad de prórroga de 10 años renovable, decisión que debe tomarse 6 meses antes de expirar el plazo, y controlada por el Parlamento federal. Pero incluso con prórrogas, nunca más de 100 años. Este esquema es más generoso que el español en plazos base (50 vs 60 para *top secret*, 30 vs 35 para *secret*; 20 vs 7-9 para *confidencial*, por lo que aquí España es mucho más breve para confidencial). Sin embargo, permite prórrogas múltiples de 10 años hasta 100 para los muy secretos, lo que es más laxo que España que solo deja una prórroga. Equilibra con supervisión parlamentaria: la autoridad concernida debe justificar la prórroga ante una comisión y esta supervisión legislativa da más garantía.

A su vez, Bélgica en 2019 creó un *Archives Commission* (Comisión de archivos de Estado) para mediar entre la seguridad y la investigación histórica. Y ha firmado acuerdos bilaterales (como con España en 2015 sobre intercambio de información clasificada) que exigen reciprocidad en protección, lo que los belgas consideraban cumplido con su Ley 1998[20].

19. DATOSMACRO-EXPANSIÓN, «Índice de Derecho a la Información. Año 2022», en *Datosmacro.com*, 2022. Disponible en: https://datosmacro.expansion.com/estado/indice-derecho-informacion?anio=2022

20. ARCHIVES GÉNÉRALES DU ROYAUME (BÉLGIQUE), *Déclassification obligatoire des documents classifiés (loi du 11 septembre 2022)*, Archives générales du Royaume, 29 de

## 6. Conclusiones

La inminente aprobación de la Ley de Información Clasificada de 2025 marcará un hito en el ordenamiento español, al derogar definitivamente la vetusta Ley de Secretos Oficiales de 1968 y sustituirla por un marco legal acorde con los valores democráticos y las necesidades de seguridad del siglo XXI. A modo de síntesis, podemos extraer las siguientes conclusiones principales de todo lo expuesto:

a) Equilibrio renovado entre seguridad y transparencia: La nueva ley supone un reequilibrio del péndulo que durante décadas estuvo inclinado hacia el secretismo. Sin menoscabar la obligación del Estado de proteger información sensible, se establecen límites temporales y materiales a esa protección, de forma que el derecho a la información y la memoria colectiva recuperan terreno. La clasificación de asuntos será excepcional, motivada y acotada en el tiempo, lo que robustece el principio democrático de publicidad de la actuación pública. España, así, normaliza su legislación situándola en la órbita de las democracias comparadas, donde los secretos oficiales tienen fecha de caducidad y control.

b) Fin de la anacrónica Ley franquista: La derogación de la Ley 9/1968 era no solo un imperativo jurídico (por su evidente desajuste con la Constitución), sino también simbólico. Con su sustitución por una ley elaborada en democracia, España se sacude otra rémora del pasado autoritario. La obra legislativa de la Transición queda por fin completada en este ámbito, cumpliendo una promesa largamente postergada. Esto contribuirá, asimismo, a cerrar heridas históricas al posibilitar la apertura de archivos relativos al régimen franquista y la transición, iluminando zonas oscuras de nuestra historia reciente con la luz de la verdad documental.

c) Avances sustanciales: Entre las mejoras palpables del nuevo régimen destacan: la creación de cuatro niveles de clasificación claros y armonizados internacionalmente (Alto Secreto, Secreto, Confidencial, Restringido); la fijación de plazos máximos de reserva (de 5, 9, 35 y 45 años según el nivel, con única prórroga en los niveles superiores); la instauración de la desclasificación automática al vencer dichos plazos; la posibilidad de revisión judicial de las clasificaciones a instancia de parte interesada; y la prohibición de clasificar materias relativas a violaciones graves de derechos humanos. Todo ello representa un salto cualitativo respecto al marco previo, introduciendo garantías de legalidad, temporalidad y control que antes brillaban por su ausencia.

noviembre de 2022. Disponible en: https://www.arch.be/index.php?a=2022-11-29-declassification-obligatoire-des-archives-classifiees-de-la-fiction-a-la-realite&l=fr&m=actualites&r=toutes-les-actualites

d) Retos y precauciones: No obstante, la ley no está exenta de aristas que demandan cautela. En especial, el régimen sancionador previsto, con multas muy elevadas a quienes difundan información clasificada, ha generado inquietud razonable en el sector periodístico y en organismos de defensa de la transparencia. Será crucial que la aplicación de estas disposiciones se haga con respeto pleno a la libertad de información consagrada en la Constitución, ponderando el interés público de las revelaciones caso por caso. De lo contrario, existe el riesgo de desalentar el periodismo de investigación y, paradójicamente, terminar fomentando más opacidad. El legislador haría bien en perfilar durante la tramitación parlamentaria estos aspectos, quizá moderando las sanciones o introduciendo excepciones explícitas por razón de interés público y buena fe informativa, alineándose así con las mejores prácticas internacionales y las recomendaciones del Consejo de Estado.

e) Impacto positivo en el conocimiento público: Si se implementa adecuadamente, la ley redundará en un enriquecimiento del patrimonio documental público y en un acceso mucho más amplio a archivos históricos por parte de ciudadanos, investigadores y periodistas. Esto permitirá reescribir páginas de la historia de España con información fidedigna, facilitar procesos de investigación judicial (especialmente en crímenes del pasado) y fortalecer la confianza ciudadana en las instituciones al hacerlas más transparentes. Como en su día dijo un jurista, «la democracia no se debilita al mostrar sus sombras, al contrario, se fortalece al afrontarlas con verdad». En este sentido, la puesta en marcha de la desclasificación periódica será un ejercicio sano de higiene democrática y rendición de cuentas ante las generaciones futuras.

f) Convergencia con estándares internacionales: La reforma legal coloca a España en línea con las obligaciones y recomendaciones internacionales en la materia. Atiende la exhortación de la UE en materia de acceso a documentos oficiales, se ajusta a las exigencias de la OTAN en cuanto a categorización y autoridad de seguridad, y responde a la jurisprudencia de derechos humanos (TEDH, CorteIDH) que exige que la seguridad nacional no sea excusa para suprimir el escrutinio sobre violaciones a derechos fundamentales. De este modo, España mejora su imagen de país comprometido con la transparencia y el Estado de derecho. En el Índice de Derecho a la Información global, es de esperar que escalemos posiciones gracias a la consagración legislativa de plazos de desclasificación y recursos accesibles.

g) Reforzamiento de la seguridad nacional: Paradójicamente, la ley también puede fortalecer la seguridad nacional en tanto diferencia lo realmente crucial de lo accesorio. Al dotar de un marco riguroso y profesional la clasificación, los recursos de protección (humanos,

técnicos, jurídicos) podrán concentrarse en guardar los secretos cuyo descubrimiento prematuro sí representaría un peligro efectivo (por ejemplo, planes militares en curso, identidades de agentes encubiertos, etc.), en lugar de diluirse en ocultar por inercia información cuyo único «peligro» era causar incomodidad política. Una seguridad bien entendida no está reñida con la transparencia: conviven al especializar cada cual su ámbito, y esta ley delimita ese justo ámbito.

La Ley de Información Clasificada de 2025 es una reforma legislativa de gran calado y profundamente necesaria, que actualiza un pilar del ordenamiento adaptándolo a los principios constitucionales y democráticos vigentes. Sus efectos se dejarán sentir en la cultura administrativa (que deberá abrazar mayores dosis de publicidad), en la vida académica (con nuevas fuentes abriéndose), en el periodismo (llamado a seguir fiscalizando, pero ahora dentro de cauces legales más definidos) y en último término en la calidad de nuestra democracia.

## BIBLIOGRAFÍA

**Alonso de Antonio, Á. L.**, «La ley de secretos oficiales», en *FORO. Revista de Ciencias Jurídicas y Sociales. Nueva Época*, vol. 18, núm. 1, 2015.

**ARCHIVES GÉNÉRALES DU ROYAUME (BÉLGIQUE)**, *Déclassification obligatoire des documents classifiés (loi du 11 septembre 2022)*, Archives générales du Royaume, 29 de noviembre de 2022.

**ARCHIVO GENERAL DE LA NACIÓN (COLOMBIA)**, *Guía para la calificación de la información (GIT-G-01)*, Bogotá, 2014.

**COLOMBIA**, *Constitución Política de Colombia*, Diario Oficial de Colombia, núm. 44.109, 4 de julio de 1991.

**COLOMBIA**, *Ley 1712 de 2014, de 6 de marzo, por la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones*, Diario Oficial de Colombia, 6 de marzo de 2014.

**DATOSMACRO-EXPANSIÓN**, «Índice de Derecho a la Información. Año 2022», en *Datosmacro.com*, 2022.

**Díaz Matey, G.**, **Cremades Guisado, Á.**, «Los secretos oficiales en España: un dilema entre transparencia y seguridad nacional», en *Gladius et Scientia. Revista de Seguridad del CESEG*, núm. 1, 2019.

**EL CONFIDENCIAL**, «El Consejo de Estado pide revisar la ley de información clasificada y alerta sobre las sanciones a periodistas», en *El Confidencial*, 15 de julio de 2025.

**ESPAÑA**, *Ley 20/2022, de 19 de octubre, de Memoria Democrática*, Boletín Oficial del Estado, núm. 252, 20 de octubre de 2022, p. 144186-144257.

**ESPAÑA**, *Ley 9/1968, de 5 de abril, sobre secretos oficiales*, Boletín Oficial del Estado, núm. 84, 6 de abril de 1968.

**ESPAÑA. CORTES GENERALES. CONGRESO DE LOS DIPUTADOS**, *Proyecto de Ley de Información Clasificada*, Boletín Oficial de las Cortes Generales. Serie A. Proyectos de Ley, núm. 65-1, 29 de agosto de 2025.

**García de Paredes Dupuy, A.**, «¿En qué consiste la Ley de Secretos Oficiales de España?», en *LISA News*, 1 de febrero de 2023.

**GOBIERNO DE ESPAÑA**, *Referencia del Consejo de Ministros. Rueda de prensa del Consejo de Ministros, 22 de julio de 2025*, La Moncloa, 22 de julio de 2025.

**González, M.**, «La reforma de la ley franquista de secretos oficiales inicia por tercera vez su tramitación en el Congreso tras dos intentos frustrados», en *El País*, Madrid, 27 de febrero de 2024.

**MÁS INFORMACIÓN, MÁS DERECHOS**, «¿Cuáles documentos son secretos en Colombia?», en *Más información, más derechos*, 31 de julio de 2014.

**Rey Martínez, F.**, «Derecho de acceso a la información y secretos oficiales en el ordenamiento español», en *Cuadernos Manuel Giménez Abad*, núm. 5, 2013.

**RTVE**, «De 30 a 75 años: la importancia de la información marca el plazo para revelar secretos oficiales en diversos países», en *RTVE Noticias*, 1 de agosto de 2022.

**Malalana Ureña, A.**, **Moreno Pérez, L.**, «La Ley de Secretos Oficiales, lastre para la investigación histórica», en *Ayer*, núm. 110, 2018.

# EL CONTROL DE LOS GASTOS RESERVADOS DEL CNI: ANÁLISIS JURÍDICO-PENAL A LA LUZ DE LA LEY 11/1995

**Carlos Álvaro Peris**
*Doctorando en Derecho*
*Universidad de Valencia*

## 1. Introducción

La gestión del dinero público siempre ha sido (y será) uno de los temas más debatidos en nuestra sociedad. El erario existe, entre otras cosas, gracias a las contribuciones que todos los ciudadanos realizamos vía impuestos. Por tanto, todo ciudadano parece estar legitimado a exigir al Estado información acerca de cómo y en qué se gasta el dinero que él ha aportado. En principio, vivimos bajo un sistema democrático que adopta los principios de un Estado de derecho. De esta manera, no es que el ciudadano pueda exigir dicho conocimiento, sino que más bien parece ser el Estado quién tiene un deber de informar a este acerca del gasto público.

Ahora bien, imaginemos que dicha información pudiera comprometer la seguridad y defensa del propio Estado. Tal vez, en ese caso, resultaría lógico y coherente no suministrar dicha información. Entonces, si permitiéramos que en esos casos las autoridades correspondientes no tuvieran que responder frente a nadie sobre cómo se ha utilizado ese dinero público, estaríamos dejando margen a la arbitrariedad y el oportunismo olvidando esos principios que caracterizan a un Estado de derecho. Por tanto, para comprender el porqué de la regulación del control de los gastos reservados, primero tendremos que abordar el conflicto entre el derecho a la libre información y la seguridad y defensa del Estado. Sin duda, nos daremos cuenta de lo difícil que resulta configurar un esquema legal dotado de los contrapesos oportunos que permitan conjugar a la vez un mínimo respeto al derecho a la libre información, junto con la protección de la seguridad y defensa del Estado.

Acto seguido, llevaremos a cabo el análisis del marco jurídico-normativo del control de los gastos reservados del Centro Nacional de Inteligencia (de

ahora en adelante, CNI). Para ello, si bien analizaremos por completo la Ley 11/1995, de 11 de mayo, reguladora de la utilización y control de los créditos destinados a gastos reservados, también necesitaremos hacer referencia a ciertos aspectos de la de la Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia y la Ley Orgánica 2/2002, de 6 de mayo, reguladora del control judicial previo del Centro Nacional de Inteligencia, con el objetivo de comprender adecuadamente las peculiaridades del marco normativo en el que opera el CNI. En materia de fondos reservados, podremos corroborar la existencia de ciertas redundancias entre la Ley 11/1995, de 11 de mayo, y la Ley 11/2002, de 6 de mayo, en relación al carácter secreto y al establecimiento de alguno de los contrapesos a los que aludíamos anteriormente. Sobre estos mecanismos de control, cabrá no solo analizar su régimen jurídico, sino también su eficacia práctica para conjugar ese equilibrio entre el derecho a la libre información y la seguridad y defensa del Estado.

Respecto a la tutela penal, estudiaremos brevemente cómo se protege la correcta gestión de los gastos reservados castigando a aquella autoridad o funcionario público, por un delito de malversación, cuando los administre de forma inadecuada, bien apropiándose de los mismos o dándoles un uso privado o un destino público distinto del establecido. Para ello, tendremos que analizar si las personas con competencias para gestionar y administrar los fondos reservados encajan en el concepto de autoridad y funcionario público, establecido en el artículo 24 del Código Penal, así como si dichos fondos reservados encajan en el nuevo concepto de patrimonio público del artículo 433 ter del Código Penal. A su vez, haremos un breve análisis sobre si estas autoridades o funcionarios públicos, encargados de gestionar y administrar los fondos reservados, también pueden llegar a cometer un delito de enriquecimiento ilícito, puesto que como veremos el legislador ya parecía contemplar la posibilidad de que existieran estas conductas arbitrarias y oportunistas en la redacción de la Ley 11/1995, de 11 de mayo.

## 2. El conflicto entre el derecho a la libre información y la seguridad y defensa del estado

La publicidad y transparencia de los gastos públicos constituye uno de los principales símbolos de un Estado de derecho. Los ciudadanos vemos cómo dicha entidad nos quita una parte de los frutos de nuestro trabajo, ahorro e inversión. Todo ello, bajo la premisa de que este dinero se nos devolverá en forma de bienestar a través de la prestación de distintos servicios públicos, como sanidad, educación o seguridad y defensa. Por tanto, parece más que razonable que el Estado justifique públicamente en qué se ha gastado ese dinero, con el objetivo de que los ciudadanos podamos evaluar si los gobernantes actuales están llevando a cabo una gestión del patrimonio público acorde con nuestros intereses o ideales políticos. Sin embargo, cuando hablamos del dinero que el Estado se gasta en materia

de inteligencia, los estándares de publicidad y transparencia se rebajan motivadamente[1].

La inteligencia trata de recopilar y analizar información que pueda ser útil para hacer frente a aquellas amenazas que comprometen la seguridad e integridad del estado, así como su naturaleza democrática[2]. Adquiere especial relevancia el secreto de estas labores para asegurar su éxito[3]. Pensemos que ya existen sectores doctrinales que se están empezando a plantear la influencia indirecta que los servicios de inteligencia pueden ejercer sobre la Corte Penal Internacional, a través del Consejo de Seguridad de las Naciones Unidas[4]. Por tanto, la inteligencia influye en muchísimos ámbitos y juega un papel trascendental para la seguridad e integridad del Estado, motivos suficientes para justificar la necesidad del secreto de sus operaciones. Además, tal y como planteaba Bobbio, el secreto es compatible con la democracia siempre y cuando sea excepcional[5].

Ahora bien, por mucho que la inteligencia pueda constituir una de esas excepciones, no puede suponer tampoco el total abandono de los principios de un Estado de derecho respecto a la transparencia y publicidad en las actuaciones de los poderes públicos. El conflicto se encuentra aquí entre el derecho a la libre información y la seguridad y defensa del Estado que podrían verse afectadas si este derecho no tuviera ningún límite al suministrar la información acerca de las operaciones de inteligencia.

Por una parte, el artículo 20.1 de la Constitución Española expresa lo siguiente: «Se reconocen y protegen los derechos: (...) d) A comunicar o recibir libremente información veraz por cualquier medio de difusión. La ley regulará el derecho a la cláusula de conciencia y al secreto profesional en el ejercicio de estas libertades». De esta manera, la Constitución Española (de ahora en adelante, CE) establece el derecho a la libre información como un derecho fundamental, pudiendo acudir así ante una vulneración del mismo a la figura del recurso de amparo. Por otra parte, el artículo 105 CE establece lo siguiente: «La ley regulará: (...) b) El acceso de los ciudadanos a los archivos y registros administrativos, salvo en lo que afecte a la seguridad y defensa del Estado, la averiguación de los delitos y la intimidad de las personas». Así, podemos comprobar cómo es la propia Constitución la que reconoce la particularidad de las actuaciones en materia de seguridad y defensa del Estado.

---

1. Martínez Vázquez, F., «El control parlamentario de los secretos oficiales», en *Revista de las Cortes Generales*, núm. 104, 2018, pág. 399.
2. Troy, T., «The «correct» definition of intelligence», en *International Journal of Intelligence and Counterintelligence*, vol. 5, 2008, pág. 433.
3. Ídem.
4. González López, D., «La influencia de la inteligencia en el Derecho Penal Internacional», en *Revista del Instituto Universitario de Investigación en Criminología y Ciencias Penales de la UV (ReCrim)*, núm. 33, 2025, págs. 54-74.
5. Bobbio, N., *Il Futuro della Democracia*, Einaudi Editore, Torino, 1991, pág. 20.

Por tanto, si bien se reconoce constitucionalmente el derecho de los ciudadanos a recibir información libremente y acceder a los archivos y registros administrativos, así como se obliga a las Administraciones Públicas a regirse por el principio de transparencia en sus actuaciones[6], se obliga constitucionalmente a que este derecho de los ciudadanos y deber de las Administraciones públicas se limite en torno a todo aquello que pueda comprometer la seguridad y defensa del Estado. Este equilibrio entre el derecho a la libre información y la seguridad y defensa del Estado quedó ratificado a nivel jurisprudencial con la STC 51/1985, de 10 de abril (ECLI:ES:TC:1985:51) en la que el Tribunal Constitucional afirmaba que «Una y otra línea del derecho -las noticias y las opiniones- encuentran un límite indiscutible en la seguridad exterior e interior del Estado». Asimismo, a nivel doctrinal, García-Trevijano Garnica afirmaba que de la regulación de los artículos 20.1 d) y 105 b) CE puede afirmarse que las Administraciones Públicas no es que no tengan el deber de informar, sino que tienen el deber de no hacerlo, es decir, de no suministrar información que pueda comprometer la seguridad y defensa del Estado[7].

Por todo ello, podemos concluir que, a primera vista, la configuración del sistema legal español parece cumplir con los estándares de un Estado democrático de derecho. Si bien existe un reconocimiento férreo del derecho a la libre información, así como una serie de garantías que puedan asegurar la eficacia de dicho derecho (entre ellas el recurso de amparo mencionado anteriormente), permite que en materia de seguridad y defensa del Estado pueda hacerse una excepción. Todo ello, con el objetivo de mantener cierto secreto en torno a distintas operaciones, como las de los servicios de inteligencia, que no podrían desempeñar adecuadamente su labor si se vieran obligados a cumplir con los mismos estándares de transparencia y publicidad que el resto de las Administraciones Públicas.

## 3. Marco jurídico-normativo

A continuación, analizaremos el marco jurídico-normativo de los gastos reservados del CNI, con la finalidad de comprobar si se cumple con ese equilibrio entre el respeto al derecho a la libre información y la seguridad y defensa del Estado, tanto desde un plano formal como material. Pese a que

6. Este mandato constitucional puede verse reflejado en el ordenamiento administrativo a través del artículo 3.1 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, en el que se obliga a que las Administraciones públicas respeten una serie de principios (entre ellos el de transparencia en las actuaciones administrativas), así como con la Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno, en la que se obliga a dichas Administraciones públicas a implementar y respetar una serie de medidas con el objetivo de conseguir la materialización de estos derechos y principios.

7. García-Trevijano Garnica, E., «Materias clasificadas y control parlamentario», en *Revista Española de Derecho Constitucional*, núm. 48, 1996, pág. 148.

la normativa más relevante para el objeto de estudio es la Ley 11/1995, de 11 de mayo, reguladora de la utilización y control de los créditos destinados a gastos reservados, tendremos que destacar también ciertos aspectos de la Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia y la Ley Orgánica 2/2002, de 6 de mayo, reguladora del control judicial previo del Centro Nacional de Inteligencia, con el fin de establecer correctamente el marco jurídico-normativo en el que puede operar, en materia de gastos reservados, el Centro Nacional de Inteligencia.

## 3.1. Autonomía del CNI

En relación con la Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia, establece cuestiones esenciales como son los principios (artículo 2), la programación de objetivos (artículo 3), funciones (artículo 4), actividades (artículo 5) ... Sin embargo, en lo relativo a gastos reservados, resulta relevante el artículo 7 que establece la «Organización» del CNI aclarando que, pese a estar adscrito al Ministerio de Defensa, a nivel orgánico, «su régimen económico-presupuestario se desarrolla en régimen de autonomía funcional bajo la figura de Organismo público con personalidad jurídica propia y plena capacidad de obrar». Esto concuerda con el régimen jurídico establecido en el artículo 8. Concretamente, en su apartado 2 se señala que «El Centro Nacional de Inteligencia elaborará anualmente un anteproyecto de presupuesto y lo elevará al Ministro de Defensa para remisión al Consejo de Ministros, que lo integrará en los Presupuestos Generales del Estado para su posterior remisión a las Cortes Generales». Le corresponde al director del CNI aprobar el anteproyecto de presupuesto, de acuerdo con el artículo 9.2 b). Asimismo, en el apartado 5 del artículo 8, se autoriza al CNI a que disponga «del 18 por 100 del total de los créditos del capítulo destinado a gastos corrientes en bienes y servicios de su Presupuesto de Gastos vigente en cada momento, en concepto de anticipo de caja fija». En el apartado 6 del mismo artículo se le autoriza a que disponga «del 2,5 por ciento del total de los créditos del capítulo de inversiones reales de su Presupuesto de Gastos vigente en cada momento, en concepto de anticipo de caja fija para las adquisiciones de material y servicios complementarios en el exterior».

Desde nuestro punto de vista, para que exista la «autonomía funcional» a la que hace referencia el artículo 7 de dicha ley se requiere, a su vez, de cierta autonomía presupuestaria, puesto que carecería de sentido reconocerle el derecho a autogestionarse, sin que exista la posibilidad de obtener el presupuesto necesario para poder ejecutar dicha autogestión. Desde un plano formal, teniendo en cuenta la organización que establece el artículo 7 y el régimen jurídico del artículo 8, podríamos confirmar la existencia de dicha autonomía. De hecho, tal y como contempla el artículo 8.3 de la misma ley, «El Gobierno establecerá las peculiaridades necesarias que garanticen su autonomía e independencia funcional». Por tanto, el Gobierno está obli-

gado a garantizar la independencia del CNI. Aunque, tal y como analizaremos a continuación, los gastos reservados tienen una serie de peculiaridades que los diferencian del resto del presupuesto público destinado al CNI.

## 3.2. Concepto y naturaleza de los gastos reservados

En primer lugar, el artículo 1 de la Ley 11/1995, de 11 de mayo, reguladora de la utilización y control de los créditos destinados a gastos reservados, establece el concepto de dichos gastos exponiendo que «Tienen la consideración de fondos reservados los que se consignen como tales en las Leyes de Presupuestos Generales del Estado y que se destinen a sufragar los gastos que se estimen necesarios para la defensa y seguridad del Estado». Por tanto, aquí el legislador ya nos está diciendo que dentro del concepto de fondos reservados solo pueden entrar aquellos que formalmente se encuentren dentro de esa partida presupuestaria contemplada en la Ley de Presupuestos Generales del Estado y que materialmente se destinen a sufragar los gastos necesarios para la defensa y seguridad del mismo. De esta manera, toda cuantía monetaria que provenga de dicha partida presupuestaria y se destine a tal fin encajará en el concepto de fondos reservados.

Respecto a su naturaleza, el mismo artículo 1 de esta Ley expone que «Dichos gastos se caracterizan respecto a los demás gastos públicos por la prohibición de publicidad y por estar dotados de un especial sistema de justificación y control». En relación con el especial sistema de justificación, el artículo 5 de dicha Ley permite que los acuerdos de autorización, compromiso de gastos y reconocimiento de obligaciones, así como la expedición de las correspondientes propuestas de pago, que hayan de realizarse con cargo a los créditos de gastos reservados, no requieran de justificación documental. Además, el artículo 3 les otorga la calificación de secreto, de acuerdo con las leyes vigentes en materia de secretos oficiales, a toda la información relativa a los créditos destinados a gastos reservados, así como la correspondiente a su utilización efectiva. Cabe resolver ahora la cuestión acerca de cuáles son los organismos que pueden disponer de dichos fondos reservados.

El artículo 4 concreta que «Sólo podrán consignarse créditos destinados a gastos reservados en los Ministerios de Asuntos Exteriores y Cooperación, Defensa, Interior y en el Centro Nacional de Inteligencia dependiente del Ministerio de la Presidencia». Entonces, podemos observar que el CNI, en materia de organización y estructura orgánica, se adscribe al Ministerio de Defensa, tal y como reconoce el artículo 7.1 de la Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia. En cambio, en materia de gastos reservados, el artículo 4.1 de la Ley 11/1995 establece al CNI como dependiente del Ministerio de la Presidencia. Esta aparente discordancia normativa cobrará sentido cuando analicemos los controles administrativos y parlamentarios de los fondos reservados, puesto que se obliga a los titulares de los Departamentos Ministeriales a realizar distintos encomendamientos.

Dado que el ministro de Defensa ya debe realizar las labores de justificación y control correspondientes a los fondos reservados concedidos a su Ministerio, puede resultar coherente y pertinente que dichas labores de justificación y control, correspondientes a los fondos reservados otorgados al CNI, sean competencia de otro ministro distinto. Todo ello, porque comprobaremos que los titulares de dichos Departamentos Ministeriales tendrán, entre otras, la competencia para dictar normas internas que aseguren el correcto destino de los fondos reservados. De esta manera, para evitar un posible conflicto de intereses, consideramos apropiada la decisión que tomó el legislador de otorgar, en materia de gastos reservados del CNI, la competencia al titular de un Departamento Ministerial que no disponga de otros fondos reservados, como es en este caso el ministro de la Presidencia.

Por tanto, hemos establecido que los fondos reservados no solo son secretos, sino que además su publicidad está prohibida y están dotados de un sistema especial de justificación y control. Todas estas características vienen a confirmar la idea que sostenía Troy acerca de cómo el secreto o no de las operaciones de inteligencia condiciona el éxito o fracaso de las mismas[8]. Ahora bien, esto no quiere decir que dichas operaciones y su correspondiente financiación deban suponer un espacio ajeno a los principios y valores de un Estado de derecho que inspiran nuestro ordenamiento jurídico. Tal y como planteaba Whitaker, la existencia de organismos de inteligencia, indispensables en un Estado democrático, exige disponer de mecanismos políticos de control, por parte de los poderes públicos, con el propósito de impedir que estas organizaciones ejecuten actuaciones arbitrarias que se aparten de su función primordial: la protección de la seguridad del Estado y la garantía del carácter democrático de sus instituciones[9]. Por ello, de acuerdo con estas ideas, la Ley 11/1995, de 11 de mayo, prevé un control administrativo interno, así como un control parlamentario, con el objetivo de asegurar el correcto uso y destino de los fondos reservados.

## 3.3. Control administrativo

La exposición de motivos nos dice que el primer mecanismo hace referencia a un control administrativo interno que respeta la peculiaridad de los gastos reservados a la vez que asegura su correcto uso. Concretamente, especifica que este «prevé procedimientos específicos de control administrativo y justificación de los gastos reservados, que aseguran que son exclusivamente destinados a las finalidades específicas para las que fueron aprobados y, al mismo tiempo, garantizan la salvaguarda del secreto y la seguridad de las actuaciones y de las personas que en ellas participan».

8. Troy, T., «The «correct» definition of intelligence», *op. cit.*

9. Whitaker, R., *El fin de la privacidad: cómo la vigilancia total se está convirtiendo en realidad*, Paidós, Barcelona, 1999, pág. 17.

La primera medida podemos encontrarla en el artículo 4.2 de la Ley 11/1995, de 11 de mayo, cuando se obliga a que los titulares de los Departamentos Ministeriales con asignación de fondos reservados informen periódicamente al presidente del Gobierno sobre la utilización de los mismos. Ahora bien, este informe no responde meramente a una cuestión de legalidad, sino que se trata de comprobar cuál está siendo la eficiencia y la eficacia del CNI para optimizar los recursos asignados, así como en el cumplimiento de los objetivos de inteligencia establecidos por el Gobierno[10]. Seguidamente, el artículo 6 de dicha Ley obliga a que los titulares de los Departamentos Ministeriales establezcan las normas internas que consideren necesarias para asegurar que los fondos reservados: 1) tan solo son utilizados por las autoridades del Estado a quienes se les asignen; y 2) únicamente para financiar las actividades señaladas en el artículo 1 de esta Ley, es decir, todas aquellas encaminadas a garantizar la seguridad y defensa del Estado.

Además, dentro de este control, considerado por la Ley 11/1995, de 11 de mayo, como administrativo interno, podríamos ubicar la figura del Interventor de la Administración General del Estado. El artículo 8.3 de la Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia, establece que «El control de la gestión económico-financiera se efectuará con arreglo a lo dispuesto en la Ley General Presupuestaria». Los artículos 157 y 158 de dicha Ley obligan a que el CNI esté sometido a un control financiero permanente. Por este motivo, existe una Intervención Delegada en el CNI encargada de controlar permanentemente la gestión presupuestaria, con la finalidad de verificar que tal gestión económico-financiera se adecua a los principios de legalidad, economía, eficiencia y eficacia[11].

También, el director del CNI debe formular las Cuentas Anuales, en el plazo de tres meses desde la conclusión del ejercicio, en los términos del artículo 127 y ss. de la Ley General Presupuestaria para ponerlas a disposición del Interventor Delegado en el CNI. Si bien, en relación a los fondos reservados, el papel de dicho Interventor se limita a emitir un informe sobre las normas internas que los titulares de los Departamentos Ministeriales establecen para asegurar el correcto uso de los fondos procedentes de los créditos de gastos reservados utilizándose únicamente por las autoridades asignadas y para los fines previstos por la ley. Por tanto, cabe entender aquí que el Interventor Delegado debe dar en su informe el visto bueno a dichas normas internas para que posteriormente sean dictadas por el titular del Departamento Ministerial correspondiente.

De esta manera, cabe ahora plantearse si esta serie de medidas suponen un control administrativo suficiente, teniendo en cuenta las particularidades

10. Jiménez-Pérez, D., «Legitimidad y control del Centro Nacional de Inteligencia», *Grupo de Estudios en Seguridad Internacional*, Universidad de Granada, 2019, pág. 3.

11. Moret Millás, V., «El Centro Nacional de Inteligencia: Una aproximación a su régimen jurídico», en *Revista Foro, Nueva época*, núm. 2, 2005, pág. 286.

de los fondos reservados. Para ello, cabe recordar que al director del CNI, con rango de Secretario de Estado, le corresponde «impulsar la actuación del Centro y coordinar sus unidades para la consecución de los objetivos de inteligencia fijados por el Gobierno», tal y como expone el artículo 9.1 de la Ley 11/2002, de 6 de mayo. Asimismo, este se ve asistido por el secretario general del CNI, con rango de Subsecretario, desempeñando todas las funciones que le establece el artículo 10 de esta misma Ley. Ambos representan así dos figuras importantes en la estructura del CNI ostentando cada uno cierto grado de responsabilidad.

Existe un primer control administrativo como son las normas internas que fija cada titular del Departamento Ministerial correspondiente para el correcto uso de los fondos reservados, previo informe del Interventor de la Administración General del Estado. Por tanto, aquí ya tenemos una primera capa de control, puesto que las autoridades que pueden disponer de estos fondos, así como las actividades a las que podrán destinarlos, vendrán fijadas por esas normas internas que habrá establecido el titular del Departamento Ministerial correspondiente. Además, el artículo 103 de la Constitución Española y el artículo 3 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, establecen que las Administraciones Públicas actuarán de acuerdo a diversos principios, entre los que se encuentra el principio de jerarquía. Por ello, carecería de sentido mantener al margen en esta materia a la persona con mayor rango dentro del escalafón del poder ejecutivo. De esta manera, se establece otra capa de control obligando a que los titulares de dichos Departamentos Ministeriales informen periódicamente al presidente del Gobierno.

Aun así, al tratarse de dinero público recaudado gracias al trabajo y esfuerzo de todos los ciudadanos, parece que los estándares democráticos nos exijan establecer alguna otra capa de control. Ahora bien, si nos damos cuenta las capas de control que hemos mencionado hasta ahora, todas dependen de personas que forman parte del propio poder ejecutivo. Por esta razón, ese plus de control que merecen los fondos reservados, al ser dinero público, debería quedar en manos de alguien que no esté implicado en dicho poder ejecutivo y que pueda representar al conjunto de los ciudadanos, siempre y cuando se consiga perjudicar lo menos posible el secreto de dichas operaciones para no comprometer la seguridad y defensa del Estado. Por ello, el legislador decidió establecer un control parlamentario de los fondos reservados con las particularidades que estudiaremos a continuación.

## 3.4. Control parlamentario

La teoría de la separación de poderes siempre ha generado cierto debate acerca de la independencia de cada poder respecto de los otros, así como de la posible superposición de uno sobre otro. Por ello, el Constituyente tuvo que confeccionar un ordenamiento jurídico dotado de los suficientes contra-

pesos entre los distintos poderes, con el objetivo de que cada uno pudiera desempeñar sus correspondientes funciones sin que ninguno de los otros se inmiscuyera arbitrariamente en sus actividades. Como siempre, desde un plano teórico, resulta una idea conceptual adecuada, coherente y plausible. Sin embargo, en la práctica hemos llegado a transitar por zonas grises en las que alguno de los poderes no solo se ha atrevido a cuestionar las actividades de otro, sino que incluso ha tratado de influenciarlas y condicionarlas o dejarlas sin efecto. Por ello, resulta esencial la defensa de aquellos mecanismos que operan como un contrapeso frente a la posible arbitrariedad de un determinado poder.

Respecto al CNI, aparte de los controles comentados anteriormente, la Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia, establece en su Capítulo III «Del Control», dos controles adicionales: 1) Control parlamentario y 2) Control judicial previo. En relación a este último, tan solo destacaremos que se encuentra regulado por la Ley Orgánica 2/2002, de 6 de mayo, reguladora del control judicial previo del Centro Nacional de Inteligencia, y que se encarga principalmente de obligar a que el CNI, en todas aquellas actividades que puedan afectar a la inviolabilidad del domicilio y al secreto de las comunicaciones, deba solicitar previamente una autorización judicial al Magistrado del Tribunal Supremo competente para poder llevarlas a cabo. Si bien puede llegar a resultar un contrapeso necesario, no ha estado exento de críticas[12]. Dado que no resulta especialmente relevante para la materia de fondos reservados no nos detendremos más en él.

La Ley 11/1995, de 11 de mayo, regula en su artículo 7.1 el sometimiento de los fondos reservados a un control parlamentario. Concretamente, explicita lo siguiente: «los créditos destinados a gastos reservados estarán sujetos al control del Congreso de los Diputados, a través de una Comisión parlamentaria compuesta por el presidente de la Cámara, que la presidirá, y aquellos Diputados que, de conformidad con la normativa parlamentaria, tengan acceso a secretos oficiales». A su vez, cabe destacar que esta misma Comisión no solo sirve para controlar los gastos reservados, sino también para que el parlamento conozca las actividades que ha llevado a cabo el CNI. Así lo establece el artículo 11.1 de la Ley 11/2002, de 6 de mayo, cuando expone que «El Centro Nacional de Inteligencia someterá al conocimiento del Congreso de los Diputados, en la forma prevista por su Reglamento, a través de la Comisión que controla los créditos destinados a gastos reservados, presidida por el Presidente de la Cámara, la información apropiada sobre su funcionamiento y actividades...».

Aun así, cabe recordar la difícil tarea de conjugar en un mismo esquema legal el derecho de los ciudadanos a controlar en qué se gasta su dinero con

12. González Cussac, J. L., «Intromisión en la intimidad y CNI. Crítica al modelo español de control judicial previo», en *Inteligencia y Seguridad: Revista de análisis y prospectiva*, núm. 15, 2014, págs. 151-186.

la protección de la seguridad y defensa del Estado. Por ello, esta Comisión está sujeta a distintas particularidades. Las sesiones son siempre secretas y sus miembros están obligados a no divulgar ni las deliberaciones ni la información obtenida, conforme al artículo 11.1 de la Ley 11/2002, el artículo 7.3 de la Ley 11/1995 y el artículo 16 del Reglamento del Congreso de los Diputados. Además, en el artículo 3 de la Ley 11/2002 se expone que la información respecto a los gastos reservados y su utilización efectiva tendrá la calificación de secreto, de acuerdo con las leyes vigentes en materia de secretos oficiales. No solo eso, sino que en el artículo 11.3 de la Ley 11/2002 se vuelve a insistir en que «Los miembros de la Comisión correspondiente estarán obligados, en los términos del Reglamento del Congreso de los Diputados, a guardar secreto sobre las informaciones y documentos que reciban».

Por tanto, podemos apreciar claramente un especial énfasis del legislador en proteger el secreto de las actividades del CNI, sobre todo en materia de gastos reservados, con el objetivo coherente de no comprometer el éxito de las mismas. Si bien podría criticarse cierta redundancia entre la Ley 11/1995 y la Ley 11/2002, respecto a la regulación de dicha Comisión, podría justificarse en ese especial énfasis que pretendía mostrar el legislador sobre la importancia de mantener el secreto para las materias ahí tratadas. Además, veníamos comentando la idea de que en un Estado de derecho debe existir separación de poderes debiendo actuar todos dentro de los límites establecidos por la ley. Esta idea puede verse reflejada en el artículo 2 de la Ley 11/1995 cuando establece que «Los créditos destinados a gastos reservados se fijarán de forma específica para cada ejercicio económico en la Ley de Presupuestos Generales del Estado» y que «La autorización de cualquier modificación presupuestaria que suponga incremento en relación con tales créditos corresponderá a las Cortes Generales, previo informe de la Comisión prevista en el artículo 7 de esta Ley».

De esta manera, el poder ejecutivo queda supeditado a aplicar los presupuestos que ha aprobado el poder legislativo. En materia de fondos reservados, todos aquellos Departamentos Ministeriales contemplados en la Ley 11/1995, de 11 de mayo, quedan sujetos a la cuantía que se les consigna en esa Ley por dicho concepto. Todo ello, bajo las premisas de la teoría de la separación de poderes en la que consideramos que es en el parlamento (poder legislativo) dónde se encuentra verdaderamente representado el conjunto de los ciudadanos. De ahí que la decisión acerca de en qué se gasta el dinero de todos emane del parlamento. Considerándose así lógico que en el caso de que deba hacerse una modificación presupuestaria, la decisión acerca de la conveniencia o no de esta misma, dependa del mismo parlamento que aprobó esos presupuestos.

Además, en el artículo 7.2 de la Ley 11/1995, de 11 de mayo, se establece la obligatoriedad de que los titulares de los Departamentos Ministeriales que tenga consignados fondos reservados informen semestralmente a la Comisión sobre la aplicación y uso de los correspondientes fondos presupues-

tarios. Sin duda, cabe plantearse cuáles deberían ser las consecuencias de incumplir dicho mandato, puesto que en la práctica han existido largos períodos en los que la Comisión no se ha convocado[13]. No parece que esta noticia generara mucha indignación ciudadana. Desde nuestro punto de vista, la inacción de dicha Comisión supone el abandono del mecanismo o contrapeso democrático más importante sobre el control de los fondos reservados. Independientemente de las responsabilidades políticas que este hecho debería generar, cuestión que no compete a nuestro estudio, la Ley obliga a respetar una periodicidad que en ocasiones se incumple inutilizando así dicho contrapeso.

La doctrina ha llegado a afirmar que existe una relación directa entre la existencia de regímenes no democráticos y aparatos de seguridad que actúan al margen de la legalidad[14]. De ahí la importancia de que la Comisión que controla los créditos destinados a gastos reservados funcione adecuadamente, respetando los plazos exigidos por la Ley 11/1995, de 11 de mayo, así como informando sobre las actividades del CNI y el uso y destino de los fondos reservados, junto al resto de funciones y competencias asignadas. Todo ello, para conseguir no poner en peligro el excelente prestigio que existe acerca del funcionamiento de los servicios de inteligencia del Estado español. Por último, destacar que en el artículo 7.4 de dicha Ley se permite que, con carácter anual, la Comisión elaboré un informe para su remisión a los presidentes del Gobierno y del Tribunal de Cuentas. Aunque el uso del término «podrá» viene a establecer más bien una recomendación que un mandato.

En definitiva, grandes autores como Locke, Montesquieu y otros tantos, han debatido a lo largo de la historia acerca de cómo perfilar un esquema legal dotado de los contrapesos adecuados entre los distintos poderes. La tarea aumenta de dificultad cuando nos vemos obligados a incorporar a ese esquema una serie de estándares democráticos propios de nuestras sociedades modernas.

La Comisión de control de los créditos destinados a gastos reservados se encuentra compuesta actualmente por una presidenta, nueve vocales y un letrado. Si las matemáticas no nos fallan llegaríamos a la conclusión de que el control sobre los 19,8 millones de euros presupuestados para el CNI, en concepto de fondos reservados[15], y recaudados gracias al trabajo, ahorro

13. Véase más ampliamente: https://www.newtral.es/comision-secretos-oficiales/20240725/

14. Moret Millás, V., «El Centro Nacional de Inteligencia: Una aproximación a su régimen jurídico», op. cit., pág. 287.

15. Esta es la asignación presupuestaria actual en concepto de fondos reservados para el CNI conforme a la Ley 31/2022, de 23 de diciembre, de Presupuestos Generales del Estado para el año 2023. Todo ello porque el ejecutivo no pudo sacar hacia delante unos nuevos presupuestos, motivo por el que estos se vieron prorrogados tal y como establece el artículo 134.4 de la Constitución Española. A pesar de ello, parece no tener extremada importancia qué presupuestos se comprueben, ya que la partida de fondos reservados otorgada

e inversión de millones de ciudadanos, queda en manos de diez parlamentarios. Aunque es cierto que cuantos más parlamentarios tengan acceso a dicha información, existe un mayor peligro de filtración de la misma, la comparativa de los datos invita a realizar una reflexión acerca de la complejidad de conjugar el equilibrio entre el derecho a la información y la protección de la seguridad y defensa del Estado.

## 4. Posible comisión de delitos de malversación ante una incorrecta gestión de los gastos reservados

Por último, dado que los fondos reservados emanan de los Presupuestos Generales del Estado son considerados evidentemente como dinero público. Uno puede ser más o menos liberal, más o menos comunitarista, más o menos socialdemócrata... Pero la existencia de un Estado, aunque fuera mínimo, implica que este va a necesitar financiarse vía impuestos para poder llevar a cabo las funciones que tiene asignadas. Incluso aquellos que defienden un Estado mínimo en el que tan solo se encargue del uso coactivo de la fuerza, de defender el derecho a la propiedad privada y poco más, necesitaría recaudar impuestos para financiar dichas actividades. Por tanto, independientemente de la ideología política que uno pueda tener, la existencia del Estado implica que todos los ciudadanos vamos a contribuir a financiar un erario suficiente como para que este pueda prestarnos todos los servicios prometidos a cambio de dicha recaudación.

De esta manera, superadas las ideas absolutistas y adoptadas con el tiempo las demócratas, los ciudadanos comenzaron a exigir una mayor transparencia en la gestión del dinero público, como es propio en un Estado de derecho. Así, poco a poco, fueron saliendo a la luz distintos casos de corrupción en nuestras instituciones generando una cierta crisis de credibilidad en torno a cómo se gestiona ese dinero público. De todos los delitos de corrupción pública parece que, en relación al objeto de estudio, el delito de malversación sea el más relevante a analizar. La doctrina considera el delito de peculado como antecedente del delito de malversación, entendiendo así que en este último se pueden llevar a cabo tres conductas posibles: sustraer (*auferre*), destruir (*interficere*) y distraer (*vertere in rem suam*)[16]. Por tanto,

al CNI lleva congelada desde 2013. Este hecho ha recibido ciertas críticas, al tratarse de unos fondos relevantes para la actividad del CNI, tanto por el período inflacionista que hemos atravesado en los últimos años incrementando el coste de todas las operaciones como por los incrementos en otras partidas presupuestarias del gasto en Defensa y no en esta. Véase más ampliamente: https://www.sepg.pap.hacienda.gob.es/sitios/sepg/es-ES/Presupuestos/PGE/PGE2024Prorroga/Paginas/PGE2024Prorroga.aspx

16. Blecua Fraga, R., «La aplicación pública de caudales a diferente destino, como delito de malversación. (Estudio del artículo 397 del Código Penal)», en *Anuario de Derecho Penal y Ciencias Penales (BOE)*, 1985, pág. 749.

podemos entender por malversación el fenómeno que engloba aquellas conductas realizadas por autoridades o funcionarios públicos consistentes en sustraer, distraer o hacer un uso indebido del patrimonio público. Concretamente, la regulación actual del Código Penal castiga a aquellas autoridades o funcionarios públicos que se apropian del patrimonio público, le dan un uso privado o lo destinan a un fin público distinto al establecido. Por tanto, antes de analizar la posible realización de estas tres conductas cabe realizar un análisis de tipicidad planteando las dos siguientes cuestiones: 1) si las personas encargadas de gestionar los fondos reservados encajan o no en el concepto de autoridad o funcionario público; y 2) si los fondos reservados se encuentran comprendidos dentro del concepto de patrimonio público.

Respecto a la primera cuestión, el artículo 4.1 de la Ley 11/1995, de 11 de mayo, establece lo siguiente: «Sólo podrán consignarse créditos destinados a gastos reservados en los Ministerios de Asuntos Exteriores y Cooperación, Defensa, Interior y en el Centro Nacional de Inteligencia dependiente del Ministerio de la Presidencia. Corresponderá exclusivamente a los titulares de estos Departamentos, de acuerdo con sus específicas características, determinar la finalidad y destino de estos fondos y las autoridades competentes para ordenar su realización». Por tanto, quién a priori tiene la capacidad para decidir el destino de los fondos reservados son los titulares de esos Departamentos. Cabe destacar que el Código Penal establece en su artículo 24 los siguientes conceptos para autoridad y funcionario público: «1. A los efectos penales se reputará autoridad al que por sí solo o como miembro de alguna corporación, tribunal u órgano colegiado tenga mando o ejerza jurisdicción propia... 2. Se considerará funcionario público todo el que por disposición inmediata de la Ley o por elección o por nombramiento de autoridad competente participe en el ejercicio de funciones públicas».

No parece haber problema en que los ministros correspondientes encajen en el concepto de autoridad, por cuanto pertenecen a un órgano colegiado como es el Gobierno y mandan respecto de las competencias que tienen atribuidas para su correspondiente Ministerio. Respecto del CNI, tal y como hemos comentado anteriormente, el artículo 9 de la Ley 11/2002, de 6 de mayo, le otorga el rango de Secretario de Estado al Director del Centro y el artículo 10 de la misma ley le otorga el rango de Subsecretario al Secretario General del Centro. Todo ello, sumado a las competencias que les establece dicha Ley parece permitirnos afirmar que puedan encajar en el concepto de autoridad que contempla el Código Penal. Por tanto, en relación con esta primera cuestión, podemos concluir que aquellas personas encargadas de gestionar los fondos reservados encajarían con los conceptos de autoridad y funcionario público a efectos penales.

Respecto al encaje de los fondos reservados en el concepto de patrimonio público, la reforma penal de la Ley Orgánica 14/2022, de 22 de diciembre, trajo consigo un nuevo concepto de patrimonio público a efectos penales. Concretamente, el artículo 433 ter del Código Penal lo define de la siguiente

manera: «A los efectos del presente Código, se entenderá por patrimonio público todo el conjunto de bienes y derechos, de contenido económico-patrimonial, pertenecientes a las Administraciones públicas». Si bien este concepto resulta novedoso para nuestro Código Penal, no lo es tanto para el conjunto del ordenamiento jurídico español, puesto que se asemeja bastante a los ya contemplados en los artículos 49 y 72 de la Ley 7/1988, de 5 de abril, de Funcionamiento del Tribunal de Cuentas y en el artículo 5 de la ley 47/2003, de 26 de noviembre, General Presupuestaria[17].

La doctrina ha criticado la alusión del Código Penal al término «Administraciones Públicas» en lugar de «Estado», puesto que la referencia a este último como titular de un conjunto de derechos y obligaciones de contenido económico se ha interpretado como la definición completa de Hacienda Pública desde un punto de vista estático[18]. De esta manera, con la regulación actual se podría estar dejando fuera del concepto de patrimonio público el patrimonio de Organismos reguladores, Agencias y Entidades públicas empresariales, Organizaciones internacionales de Derecho público, Entidades que ejerzan potestades públicas de soberanía o administrativas o Sociedades mercantiles públicas[19]. Sin perjuicio de estos matices, podemos entender que la «nueva» definición de patrimonio público comprende cualquier tipo de bien (mueble o inmueble) o derecho que pueda ser evaluado económicamente y que sea público, es decir, perteneciente a las Administraciones Públicas[20]. Por tanto, no existe óbice a considerar el patrimonio del CNI como público, por cuanto se trata de un organismo adscrito orgánicamente al Ministerio de Defensa, tal y como señala el mencionado artículo 7.1 de la Ley 11/2002, de 6 de mayo, afirmando de esta manera la pertenencia a la Administración Pública, tal y como exige el artículo 433 ter del Código Penal. Concluimos así la existencia de una posible comisión de un delito de malversación de fondos reservados por parte de la autoridad o funcionario público competente, de conformidad con lo establecido por la doctrina[21].

---

17. González Cussac, J. L., «Delitos contra la administración pública (II): cohecho. Tráfico de influencias. Malversación. Fraudes y exacciones ilegales. Actividades prohibidas. Abusos en el ejercicio de la función pública», en González Cussac, J. L. (Coord.): *Derecho Penal. Parte Especial. 8ª edición*, Valencia, Tirant lo Blanch, 2023, pág. 771.

18. Herrero Suazo, S. en Amorós Rica, N. (Dir.), *Comentarios a las leyes tributarias y financieras*, Madrid, Edersa, 1986, pág. 12.

19. De la Mata Barranco, N. J., «La reforma de la malversación: ¿para qué?», en *Almacén de derecho*, 2023. Recuperado de https://almacendederecho.org/la-reforma-de-la-malversacion-para-que [Última Consulta: 4 de septiembre de 2025].

20. Morales Hernández, M. A., «La reforma del delito de malversación de patrimonio público en el Código Penal español: ¿Un avance o un retroceso en la lucha contra la corrupción?», en *Revista Electrónica de Ciencia Penal y Criminología*, núm. 25, 2023, pág. 9.

21. «También cabe la malversación de «fondos reservados», aunque deben tenerse en cuenta las peculiaridades que presenta la gestión de estos fondos», en Muñoz Conde, F., *Derecho Penal. Parte Especial*, 25ª edición, Valencia, Tirant lo Blanch, 2023, pág. 1018.

Una vez afirmado que los fondos reservados encajan en la definición de patrimonio público y las personas encargadas de gestionarlos pueden encajar en el concepto de autoridad o funcionario público, cabe analizar cuáles son las posibles conductas de malversación que pueden llegar a cometer en caso de llevar a cabo una incorrecta gestión de los mismos. La primera conducta hace referencia a la malversación por apropiación, tipificada en el actual artículo 432 CP y correspondiente a la acción de «sustraer» (*auferre*). A su vez, contempla dos modalidades comisivas distintas: una destinada a castigar al que, por acción, se apropia del patrimonio público y otra destinada a castigar al que, por omisión, permite que sea otro quien se apropie de dicho patrimonio público[22].

La nota esencial que la diferencia respecto de las otras tipologías o modalidades, tal y como expresa literalmente el artículo 432, es la existencia de ánimo de lucro, es decir, el sujeto realiza dicha conducta con la perspectiva de obtener una ventaja propia, o bien, para un tercero. En cambio, la segunda modalidad o tipología hace referencia a la malversación de uso o disposición, conducta tipificada en el artículo 432 bis CP y consistente en la acción de «distraer» el patrimonio público (*vertere in rem suam*) para un uso privado. En este caso, las dos notas esenciales que diferencian esta modalidad respecto de las otras dos son: 1) que responde a una finalidad de mero uso, es decir, no existe ánimo de apropiarse del patrimonio público, si no tan solo de utilizarlo, distinguiéndose así de la primera conducta del 432 CP. 2) Que esta modalidad de uso del patrimonio público responde a un fin privado y no público, distinguiéndose así de la conducta tipificada en el artículo 433 CP.

De esta manera, nos quedaría por establecer el concepto de la tercera conducta más importante de la malversación, consistente en malversar caudales públicos dándoles un uso público distinto al establecido o presupuestado. Esta modalidad de la malversación respondería también concretamente a la acción de «distraer» (*vertere in rem suam*), pero con una finalidad distinta a la de la tipología anterior. La doctrina mayoritaria, con un énfasis especial, sitúa el foco de esta modalidad de malversación en el fin público, es decir, la diferencia principal con respecto a las otras modalidades de malversación reside en que el autor dedica los caudales a un fin público, pero distinto del establecido o presupuestado[23]. Por tanto, se trata

22. González Cussac, J. L., «Delitos contra la administración pública (II): cohecho. Tráfico de influencias. Malversación...», *op. cit.*, pág. 773.

23. «No se trata aquí, por tanto, de dar una finalidad privada a los bienes públicos, definitiva o temporal, sino de un desvío presupuestario a finalidades públicas, pero distintas de las previstas» en Muñoz Conde, F., *Derecho Penal. Parte Especial*, *op. cit.*, pág. 1020. «La doctrina observó su diferencia palpable con las otras figuras de malversación, en la medida que aquí el autor dedica a un fin público, pero distinto, los caudales y no a una finalidad privada como en las otras modalidades» en González Cussac, J. L., «Delitos contra la administración pública (II): cohecho. Tráfico de influencias. Malversación...», *op. cit.*, pág. 776.

de otra conducta en la que simplemente se le da un uso (y no se apropia) al patrimonio público, diferenciándose así de la conducta del artículo 432 CP, pero ese otro uso, distinto del presupuestado o establecido, responde a otro fin público y no privado, distinguiéndose así de la conducta tipificada en el artículo 432 bis CP.

Por ello, para cometer un delito de malversación, no haría falta que esa autoridad o funcionario público se apropiara o diera un uso privado a dichos fondos reservados, sino que simplemente con que les diera un uso público distinto al de los fines establecidos en el artículo 1 de la Ley 11/1995, de 11 de mayo, («que se destinen a sufragar los gastos que se estimen necesarios para la defensa y seguridad del Estado») estaría cometiendo un delito de malversación de usos públicos distintos a los establecidos o presupuestados. A su vez, consideramos relevante destacar brevemente la posible comisión de un delito de enriquecimiento ilícito. Este delito que se recuperó con la reforma de la Ley Orgánica 14/2022, de 22 de diciembre, se encuentra tipificado en el artículo 438 bis del Código Penal de la siguiente manera: «La autoridad que, durante el desempeño de su función o cargo y hasta cinco años después de haber cesado en ellos, hubiera obtenido un incremento patrimonial o una cancelación de obligaciones o deudas por un valor superior a 250.000 euros respecto a sus ingresos acreditados, y se negara abiertamente a dar el debido cumplimiento a los requerimientos de los órganos competentes destinados a comprobar su justificación, será castigada con las penas de prisión de seis meses a tres años, multa del tanto al triplo del beneficio obtenido, e inhabilitación especial para empleo o cargo público y para el ejercicio del derecho de sufragio pasivo por tiempo de dos a siete años».

Todo ello debido a que la Disposición adicional única de la Ley 11/1995, de 11 de mayo, reguladora de la utilización y control de los créditos destinados a gastos reservados, obliga a los titulares de los Departamentos, en cuyos presupuestos figuren créditos asignados a gastos reservados, y las autoridades a ellos subordinadas que, de conformidad con lo previsto en el artículo 4, tengan acceso a la utilización de fondos procedentes de estos créditos, «efectúen ante el Presidente del Congreso de los Diputados una declaración especial sobre su situación patrimonial en la toma de posesión de sus cargos». Por tanto, con esta obligatoriedad parecía ya intuir en aquel momento el legislador que el gasto de unos fondos cuyo uso está sometido a cierta discrecionalidad podía dar lugar a conductas oportunistas. De esta forma, no existiría ningún obstáculo a reconocer la posibilidad de que dichas autoridades pudieran llegar a cometer un delito de enriquecimiento ilícito. Si bien su detección podría ser compleja, puesto que la propia Disposición adicional única limita el acceso a dicha información a la Comisión parlamentaria de control de los créditos destinados a gastos reservados. Todo ello, con el fin de mantener el esquema legal configurado por esta Ley en la que insistimos que se trata de conseguir un equilibrio adecuado entre el derecho a la libre información y la protección de la seguridad y defensa del Estado.

## 5. Conclusiones

En primer lugar, en relación con el conflicto entre el derecho a la libre información y la seguridad y defensa del Estado, queda constatado tanto el derecho de los ciudadanos a exigir un mínimo de transparencia en materia de gastos reservados como el mandato a las Administraciones Públicas de no suministrar aquella información que pueda comprometer la seguridad y defensa del Estado. Además, hemos podido comprobar cómo la jurisprudencia y la doctrina avalan dichas interpretaciones. Por tanto, el legislador trata de confeccionar un sistema legal que permita mantener el secreto de las operaciones de inteligencia, con el fin de no comprometer el éxito de las mismas, a la vez que se limite lo mínimamente indispensable aquellos derechos fundamentales que de no sufrir dicha limitación pondrían en peligro la seguridad y defensa del Estado (como es el caso del derecho a la libre información). Asimismo, la ponderación entre derechos fundamentales conforme a los principios y valores de nuestra democracia moderna supondrá una de las claves para hacer frente a los numerosos desafíos que tiene por delante el sector de la inteligencia. Entre otros muchos, la adopción masiva de sistemas de inteligencia artificial en la sociedad y las posibles vulneraciones de nuestros derechos fundamentales que este acontecimiento podría provocar[24].

Seguidamente, respecto al marco jurídico-normativo, primero constatamos la autonomía del CNI, así como el mandato existente al Gobierno para que garantice dicha autonomía. Acto seguido, hemos establecido el concepto de fondos reservados exponiendo que solo podrán tener esta consideración aquellos que se encuentren dentro de la partida presupuestaria de la Ley de Presupuestos Generales del Estado, contemplada para fondos reservados, y que materialmente se destinen a sufragar los gastos necesarios para la defensa y seguridad del Estado. Por lo que respecta a su naturaleza, los fondos reservados no solo son secretos, sino que además su publicidad está prohibida y están dotados de un sistema especial de justificación y control, confirmando así la idea sostenida acerca de la importancia del mantenimiento del secreto en las operaciones de inteligencia y su compatibilidad excepcional con un sistema democrático de derecho.

Posteriormente, hemos analizado las distintas capas de control que existen para vigilar la adecuada utilización de los fondos reservados. Respecto al control administrativo interno, se establece una obligatoriedad de que los titulares de los Departamentos Ministeriales con asignación de fondos reservados informen periódicamente al presidente del Gobierno. Además, estos mismos están a su vez obligados a establecer las normas internas que consideren necesarias para asegurar que los fondos reservados tan solo son utilizados por las autoridades del Estado a quienes se les asignen y única-

24. Álvaro Peris, C., «Inteligencia artificial y protección penal de los derechos fundamentales», en *Derecho Digital e Innovación*, núm. 22, 2024, pág. 3.

mente para financiar las actividades encaminadas a garantizar la seguridad y defensa del Estado. Ahora bien, estas medidas, más que un verdadero contrapeso y control democrático de los fondos reservados, parecen tener como finalidad la comprobación, por parte de los altos mandatarios del poder ejecutivo, de que esos fondos reservados se están utilizando en consonancia con los objetivos marcados por la Directiva de inteligencia. Por tanto, si bien sí que puede considerarse como una capa de control por cuanto la información acerca del uso de los fondos reservados se pone en conocimiento de distintas autoridades del poder ejecutivo, destaca mucho más como medida de eficacia de los objetivos de inteligencia que como mecanismo de control. Todo ello, porque es al fin y al cabo el propio poder ejecutivo el que se está controlando asimismo sobre el uso de dichos gastos.

De esta manera, en relación con la teoría de la separación de poderes, es el control parlamentario el que adquiere una especial relevancia. La Comisión de control de los créditos destinados a gastos reservados (tradicionalmente conocida como la Comisión de secretos oficiales) representa el verdadero control democrático del correcto uso de dichos fondos. Todo ello, en base a que esta Comisión está formada por parlamentarios (elegidos democráticamente por los ciudadanos) que, si bien quedan sometidos al secreto de las sesiones, en ellas controlan el uso y destino de los gastos reservados, así como el conjunto de las actividades que lleva a cabo el CNI. En definitiva, el ordenamiento jurídico español se apoya en dicha Comisión para sostener la idea de que incluso en una materia con tal nivel de exigencia respecto al secreto, como son los gastos reservados o las actividades del CNI, nuestro sistema legal ofrece un contrapeso democrático que evite la posible deriva de las autoridades responsables hacia conductas arbitrarias u oportunistas.

Cuestión diferente es que existan períodos en los que dicha Comisión no se convoque, provocando así la ruptura del esquema legal de la vigilancia de los gastos reservados al dejar inactivo el principal control democrático de los mismos. O que los ciudadanos no se sientan representados por los parlamentarios que forman dicha Comisión. Por ello, desde un plano teórico, podría decirse que existen buenas ideas en la base de la configuración legal del control de los gastos reservados. Sin embargo, la práctica nos ha mostrado la carencia de efectividad del mecanismo de control parlamentario por cuanto en el momento en el que se deja de convocar la Comisión en los plazos legalmente establecidos los gastos reservados se quedan sin ese control parlamentario. De esta manera, pretendemos dejar constancia de la necesidad de establecer mecanismos adicionales que, o bien aseguren en todo momento el funcionamiento adecuado de dicha Comisión, o bien establezcan para ese tipo de casos otro mecanismo adicional de control democrático que supla sus funciones.

Recordemos que la doctrina ha llegado a afirmar que existe una relación directa entre la existencia de regímenes no democráticos y aparatos de segu-

ridad que actúan al margen de la legalidad[25]. De ahí la importancia de que los mecanismos de control democráticos funcionen para que no se pueda poner en entredicho la excelente reputación que existe acerca de los servicios de inteligencia españoles.

Por último, respecto a las posibles responsabilidades penales de las autoridades y funcionarios públicos que gestionan y administran los fondos reservados, estos podrían llegar a cometer un delito de malversación en el caso de que se apropien de dichos fondos, les den un uso privado o un uso público distinto al establecido o presupuestado. Todo ello, tras haber confirmado el encaje de las personas que los gestionan en el concepto de autoridad o funcionario público a efectos penales, así como el encaje de los fondos reservados dentro del nuevo concepto de patrimonio público que establece el Código Penal. A su vez, estos pueden cometer, en relación a la gestión y administración de fondos reservados, un delito de enriquecimiento ilícito si habiendo obtenido un incremento patrimonial o una cancelación de obligaciones o deudas por un valor superior a 250.000 euros respecto a sus ingresos acreditados, durante el desempeño de su función o cargo y hasta cinco años después de haber cesado en ellos, se negaran abiertamente a dar el debido cumplimiento a los requerimientos de los órganos competentes destinados a comprobar su justificación, de conformidad con lo establecido en el artículo 438 bis del Código Penal.

Los servicios de inteligencia españoles continuarán prestando sus servicios de la mejor manera posible para contribuir a la seguridad y defensa de nuestro Estado. Ahora bien, ello no es óbice a que un sistema democrático que se inspira en los principios y valores de un Estado de derecho no deba defender a capa y espada el buen funcionamiento de los mecanismos que distan a las personas que ocupan los distintos poderes públicos de todo tipo de comportamiento arbitrario u oportunista. Pues como dijo Louis Brandeis: «La luz del sol es el mejor desinfectante»[26].

## BIBLIOGRAFÍA

**Álvaro Peris, C.**, «Inteligencia artificial y protección penal de los derechos fundamentales», en *Derecho Digital e Innovación*, núm. 22, 2024.

**Blecua Fraga, R.**, «La aplicación pública de caudales a diferente destino, como delito de malversación. (Estudio del artículo 397 del Código penal)», en *Anuario de Derecho Penal y Ciencias Penales (BOE)*, 1985.

25. Moret Millás, V., «El Centro Nacional de Inteligencia: Una aproximación a su régimen jurídico», op. cit.

26. Brandeis, L. D., *Other people's money and how the bankers use it*, Nueva York, Frederick A. Stokes Company Publishers, 1914.

**Bobbio, N.**, *Il Futuro della Democracia*, Einaudi Editore, Torino, 1991.

**Brandeis, L. D.**, *Other people's money and how the bankers use it*, Nueva York, Frederick A. Stokes Company Publishers, 1914.

**De la Mata Barranco, N. J.**, «La reforma de la malversación: ¿para qué?», en *Almacén de derecho*, 2023.

**García-Trevijano Garnica, E.**, «Materias clasificadas y control parlamentario», en *Revista Española de Derecho Constitucional*, núm. 48, 1996.

**González Cussac, J. L.**, «Intromisión en la intimidad y CNI. Crítica al modelo español de control judicial previo», en *Inteligencia y Seguridad: Revista de análisis y prospectiva*, núm. 15, 2014.

**González Cussac, J. L.**, «Delitos contra la administración pública (II): cohecho. Tráfico de influencias. Malversación. Fraudes y exacciones ilegales. Actividades prohibidas. Abusos en el ejercicio de la función pública», en González Cussac, J. L. (Coord.): *Derecho Penal. Parte Especial. 8ª edición*, Valencia, Tirant lo Blanch, 2023.

**González López, D.**, «La influencia de la inteligencia en el Derecho Penal Internacional», en *Revista del Instituto Universitario de Investigación en Criminología y Ciencias Penales de la UV (ReCrim)*, núm. 33, 2025.

**Gutiérrez Ayala, M.**, «El gasto público en el seno de la transparencia y rendición de cuentas. Una perspectiva argumentativa», en Revista de la Facultad de Derecho y Ciencias Sociales Benemérita Universidad Autónoma de Puebla, núm. 17, 2015.

**Herrero Suazo, S.** en **Amorós Rica, N.** (Dir.), *Comentarios a las leyes tributarias y financieras*, Madrid, Edersa, 1986.

**Jiménez-Pérez, D.**, «Legitimidad y control del Centro Nacional de Inteligencia», *Grupo de Estudios en Seguridad Internacional*, Universidad de Granada, 2019.

**Martínez Vázquez, F.**, «Repertorio bibliográfico sobre control parlamentario», en *Teoría y Realidad Constitucional*, núm. 19, 2007.

**Martínez Vázquez, F.**, «El control parlamentario de los secretos oficiales», en *Revista de las Cortes Generales*, núm. 104, 2018.

**Morales Hernández, M. A.**, «La reforma del delito de malversación de patrimonio público en el Código Penal español: ¿Un avance o un retroceso en la lucha contra la corrupción?», en *Revista Electrónica de Ciencia Penal y Criminología*, núm. 25, 2023.

**Moret Millás, V.**, «El Centro Nacional de Inteligencia: Una aproximación a su régimen jurídico», en *Revista Foro, Nueva época*, núm. 2, 2005.

**Muñoz Conde, F.**, *Derecho Penal. Parte Especial*, 25ª edición, Valencia, Tirant lo Blanch, 2023.

**Troy, T.**, «The «correct» definition of intelligence», en *International Journal of Intelligence and Counterintelligence*, vol. 5, 2008.

**Whitaker, R.**, *El fin de la privacidad: cómo la vigilancia total se está convirtiendo en realidad*, Paidós, Barcelona, 1999.

# INTELIGENCIA ECONÓMICA Y SEGURIDAD ENERGÉTICA EN LA CULTURA DE SEGURIDAD Y DEFENSA

**Alberto Camarero Orive**
*Profesor Titular de Universidad*
*Universidad Politécnica de Madrid*

## 1. Introducción

En la era contemporánea, el concepto de seguridad nacional trasciende lo puramente militar para abarcar ámbitos económicos, tecnológicos y energéticos. La seguridad energética, definida como la disponibilidad ininterrumpida de fuentes de energía a un precio asequible, se sitúa actualmente en el centro de la estrategia nacional e internacional[1]. Tras las crisis geopolíticas recientes y la acelerada transformación hacia sistemas energéticos descarbonizados, la defensa del suministro energético y la gestión de infraestructuras críticas son pilares esenciales para la resiliencia de los Estados y las organizaciones. La seguridad energética se ha constituido en una dimensión crítica de la seguridad nacional y la resiliencia estratégica, especialmente en economías avanzadas integradas y abiertas a la competencia tecnológica y geopolítica internacional[2].

En este sentido, el papel de la inteligencia económica, entendida como la disciplina que recopila, analiza y protege información estratégica, deviene fundamental para anticipar amenazas, gestionar vulnerabilidades y facilitar decisiones informadas en la cultura de defensa contemporánea, con un papel primordial en todo lo relacionado con la seguridad energética. Desde una perspectiva técnica, implica la gestión integral de ciclos inteligentes: necesidad, obtención, análisis, procesamiento, protección y retroalimentación de todo el proceso. En el ámbito energético, se ha desarrollado la inteligencia energética, especializada en la monitorización de los mercados, las

1. Véase REAL INSTITUTO ELCANO, *Inteligencia económica como vector internacional de seguridad*. Documento de Trabajo, 2022.

2. DEPARTAMENTO DE SEGURIDAD NACIONAL, *Informe Anual de Seguridad Nacional*, 2024.

tecnologías y los riesgos geopolíticos que afectan la seguridad de suministro y la competitividad.

Así, la inteligencia económica es hoy más necesaria que nunca para anticipar amenazas, optimizar la toma de decisiones y salvaguardar intereses estatales y corporativos en el sector energético. Esta simbiosis, entre inteligencia económica y seguridad energética, está transformando las culturas de defensa de los Estados modernos, articulando respuestas multidimensionales ante retos históricos y emergentes.

Con todo, la interrelación entre inteligencia económica y seguridad energética configura una nueva simbiosis conceptual, que exige el desarrollo de nuevos modelos analíticos, capacidades profesionales especializadas y herramientas tecnológicas de alto nivel.

En este capítulo se aborda, de manera general, la evolución doctrinal, los pilares metodológicos y los retos operativos de esta relación entre ambas disciplinas, con especial atención en el contexto español y europeo, pero con alcance global. La energía ya no es sólo un bien económico, es también un instrumento de poder, un factor de vulnerabilidad y la base de la autonomía estratégica, tan necesaria en el contexto geopolítico actual.

## 2. Evolución de la inteligencia económica aplicada a la seguridad energética

La crisis del petróleo de 1973, conocida como primera crisis del petróleo, marcó un hito en la conciencia estratégica de Occidente: la energía dejó de ser un mero recurso económico para convertirse en elemento estructural de la defensa y la autonomía nacional.

Francia fue pionera en institucionalizar la inteligencia económica como política de Estado, integrándola en todos los sectores críticos. Por lo que respecta a Estados Unidos, desarrolló capacidades avanzadas con la integración de inteligencia comercial, tecnológica y energética en su aparato de seguridad nacional. China, por su parte, ha elevado la vigilancia de activos claves y la protección de cadenas de valor estratégicas a pilar esencial de su proyección global[3].

Ante esta situación, la aparición de amenazas híbridas, la globalización de mercados, el auge de potencias emergentes, la digitalización de infraestructuras y la transición climática han expandido la inteligencia económica más allá de la protección empresarial, con lo que ello conlleva. Hoy, la inteligencia económica implica análisis prospectivo, vigilancia tecnológica, cooperación institucional y ciber-inteligencia en energías, redes logísticas, puertos y cadenas críticas, entro otras implicaciones.

3. Véase REAL INSTITUTO ELCANO, *Inteligencia económica..., op. cit.*; Poza Cano, D., *Energía y geoestrategia.* Ministerio de Defensa, 2024.

Así, la cultura de defensa moderna no puede disociarse de la dimensión energética, ya que la dependencia de recursos externos condiciona la capacidad operativa de cualquier nación e introduce vulnerabilidades susceptibles de ser explotadas a través de ataques híbridos, presión diplomática o estrategias hostiles. La defensa, por tanto, es indisociable de la protección de activos energéticos, la resiliencia ante shocks de mercado y la gestión de riesgos sistémicos derivados del entorno geopolítico y tecnológico[4].

## 3. El nuevo paradigma de la seguridad energética y su relación con la inteligencia económica

Durante las últimas décadas, la seguridad energética ha evolucionado de una visión restringida, fundamentalmente, al suministro de hidrocarburos a una concepción multidimensional, donde la sostenibilidad, la resiliencia, la equidad, la accesibilidad y la gobernanza convergen con los objetivos de defensa nacional[5]. El desarrollo de energías renovables, como la fotovoltaica, eólica *on/offshore*, hidrógeno verde, entre otras, y el despliegue de tecnologías de almacenamiento y digitalización del sistema eléctrico están transformado el escenario operativo del sistema energético[6].

El impacto del cambio climático y de la transición energética sobre las cadenas de suministro tecnológicas requiere incorporar a la seguridad energética criterios ecológicos y medioambientales, así como la capacidad de gestión de nuevos riesgos como la dependencia de minerales críticos (litio, cobalto, tierras raras, etc.) y la vulnerabilidad ante ciberataques a redes y sistemas industriales.

El mantenimiento de stocks, la diversificación de rutas y fuentes, la resiliencia institucional y la proactividad ante los riesgos de desinformación y manipulación del mercado son elementos esenciales de este nuevo paradigma.

Por lo que respecta a la cultura de defensa en el siglo XXI es necesariamente intersectorial: la protección de infraestructuras críticas, la gestión de recursos energéticos, la ciberdefensa de sistemas industriales y la resiliencia ante desinformación estratégica forman parte de los deberes no solo de las fuerzas armadas, sino de todo el aparato público-privado.

España, por su posición geoestratégica, integra iniciativas de concienciación, simulacros, redes de alerta, formación avanzada, doctrina OTAN

4. Véase IEEE, *La inteligencia económica en un mundo globalizado. Cuadernos de Estrategia*, núm. 162, 2021.

5. Véase Chacón Rueda, A. M., Análisis del sector energético y el crecimiento de las energías renovables, 2021.

6. Véase Bernaldo, M. O., *Transición energética sostenible. Una transición inteligente hacia un modelo energético sostenible para España en 2050*, 2021.

y gobernanza inteligente con la UE. En el debate energético, la cultura de defensa engloba ahora la equidad en el acceso, la sostenibilidad, la transición justa y la competitividad nacional. La consolidación de *hubs* logísticos, la protección de terminales y redes, y el liderazgo en energías limpias refuerzan la autonomía y la influencia en el Mediterráneo y Europa.

Así, la inteligencia energética asume aquí un papel multidisciplinar para apoyar la toma de decisiones políticas, empresariales y de defensa, facilitando una visión holística y preventiva. Pero no se debe olvidar el carácter transformador de la inteligencia económica en seguridad energética, donde no se limita a recopilar información, sino que analiza tendencias, interpreta señales débiles y elabora escenarios prospectivos.

Con todo, las funciones fundamentales de la inteligencia económica en su relación con la seguridad energética abarcan, entre otros, los siguientes aspectos:

a) Anticipación y monitorización sistemática de riesgos políticos, tecnológicos y económicos.

b) Detección de amenazas híbridas y vulnerabilidades en infraestructuras críticas.

c) Evaluación de la viabilidad y seguridad de inversiones extranjeras en sectores energéticos sensibles.

d) Análisis comparativo de la evolución de los mercados energéticos y el impacto de sanciones, conflictos armados o tensiones comerciales.

e) Identificación y seguimiento de campañas de influencia, desinformación y operaciones hostiles de actores estatales y no estatales.

Para ello, se utilizan metodologías avanzadas e instrumentos innovadores como sistemas de vigilancia tecnológica, el uso de Big Data, la inteligencia artificial para modelización de precios y demanda, la simulación de crisis y la construcción de mapas de riesgo.

Por ejemplo, las empresas energéticas multinacionales han desarrollado sistemas propios de inteligencia, que articulan las ventajas competitivas ante crisis como el suministro de gas tras la invasión rusa de Ucrania, actuando en tiempo real sobre rutas, contratos y relaciones diplomáticas, empleando sistemas *ad-hoc* para la anticipación y respuesta frente a la volatilidad de mercados, riesgos regulatorios e incidentes geopolíticos.

## 4. Diversificación estratégica, resiliencia y gestión de vulnerabilidades

La diversificación constituye un imperativo estratégico en la gestión de la seguridad energética. Supone aplicar políticas activas que permitan reducir dependencias excesivas de proveedores, tecnologías, rutas y materias primas, desarrollando un *mix* energético flexible, utilizando las energías reno-

vables, la energía hidráulica, la energía nuclear, el hidrógeno, el almacenamiento y la gestión flexible de las redes existentes.

El sector energético es blanco frecuente de ciberataques, sabotaje industrial, presión diplomática, manipulación informativa y sanciones económicas cruzadas.

Casos como el sabotaje del *Nord Stream*, los ataques a terminales petroleras, la crisis de seguridad en gasoductos y las campañas de desinformación en medios digitales han demostrado la importancia de contar con sistemas de inteligencia colaborativa, protocolos nacionales de respuesta y análisis integrado de riesgos[7].

Así, el diagnóstico y la gestión de vulnerabilidades es responsabilidad compartida entre administraciones públicas, nacionales y multinacionales, empresas, organismos reguladores y cuerpos de defensa. Las vulnerabilidades sistémicas pueden surgir de dependencias tecnológicas, fracturas sociales o debilidades institucionales[8]. Y esa ahí, donde la inteligencia económica juega un papel fundamental, detectando, analizando y proponiendo soluciones antes estas situaciones críticas. Además, los riesgos se amplifican ante amenazas híbridas, ciberataques, manipulación del mercado o presión diplomática sobre infraestructuras críticas y cadenas globales de suministro, tanto de productos energéticos como de minerales críticos o estratégicos.

Con todo, la resiliencia del sistema se considera crítica ante las vulnerabilidades del sector, basándose en una gestión activa y preventiva de las vulnerabilidades, el mapeo de riesgos críticos y la constitución de equipos multidisciplinares capaces de responder antes incidentes complejos y escenarios de crisis. Todo ello implica el desarrollo de infraestructuras robustas, protocolos de respuesta ante crisis, reservas estratégicas y mecanismos de gestión flexible que permitan la recuperación y el funcionamiento del sistema ante incidentes graves.

## 5. Nuevas fuentes de energía y retos tecnológicos

La transición energética implica la sustitución progresiva de los combustibles fósiles por fuentes limpias y sostenibles, lo cual modifica radicalmente el escenario geopolítico y tecnológico. Soluciones como el gas, el hidrógeno verde como vector energético clave debido a su potencial para almacenar energía y desacoplar los sistemas productivos de la volatilidad de los mercados fósiles, los biocombustibles, u otras tecnologías que se están desarrollando son una apuesta para el futuro de la transición energética.

---

7. Véase DEPARTAMENTO DE SEGURIDAD NACIONAL, *Informe Anual..., op. cit.*; RH ASESORES IMPROVING, *Inteligencia Energética (recurso divulgativo)*, 2025.

8. Véase Reglero, J., La importancia del sector energético en la economía, 2022; Poza Cano, D., *Energía..., op. cit.*

Paralelamente, tecnologías avanzadas como la fusión nuclear, el almacenamiento masivo, la digitalización (blockchain, IA, Big Data aplicada) y las energías renovables offshore configuran nuevos ecosistemas industriales y de seguridad, que veremos su grado de implantación en los próximos años[9].

Además, Europa y España se enfrentan a importantes retos para asegurar el acceso a minerales críticos y posicionarse en el liderazgo de mercados globales de la transición limpia. En este sentido, la conocida como diplomacia de los minerales, las alianzas regionales y el apoyo institucional son esenciales para reducir dependencias y anticipar posibles conflictos emergentes.

Estos desarrollos generan oportunidades, pero también riesgos: las cadenas de valor emergentes para baterías, paneles solares y electrolizadores suelen estar concentradas en regiones específicas y bajo control de actores geopolíticos relevantes. La competencia internacional por minerales críticos (litio, cobalto, tierras raras, etc.) impone nuevos desafíos a la autonomía estratégica de los Estados y a la seguridad de los suministros[10].

Es aquí donde la inteligencia económica debe anticipar los movimientos industriales, vigilar el desarrollo tecnológico, detectar dependencias peligrosas y analizar los flujos de inversión pública y privada en los sectores energéticos estratégicos, para garantizar nuestra seguridad energética.

Resulta imprescindible construir capacidades nacionales de I+D e impulsar la cooperación internacional regulada para minimizar vulnerabilidades y maximizar ventajas competitivas.

## 6. Cultura de seguridad y defensa: formación, cooperación y gobernanza

La verdadera consolidación de una cultura de defensa capaz de integrar la seguridad energética comienza por la profesionalización y formación avanzadas en inteligencia económica aplicada. Los responsables públicos, militares y corporativos deben comprender en profundidad los retos transversales del sector energético y tecnológico, mejorando sus habilidades de análisis, gestión y anticipación.

En este sentido, los programas de formación deben romper barreras sectoriales, promoviendo la colaboración entre las diferentes disciplinas, como la energía, la defensa, la industria, la inteligencia y los diferentes ámbitos regulatorios.

La cultura de defensa no puede limitarse al ámbito castrense, sino que debe abarcar la protección de infraestructuras críticas, la ciberdefensa, la vigilancia

9. Véase KPMG, *La IA y la transición energética: ¿aliadas estratégicas?*, 2024.

10. Véase INSTITUTE FOR GLOBAL CHANGE. *Greening AI: A Policy Agenda for the Artificial Intelligence and Energy Revolutions*, 2024.

estratégica de los mercados y la gestión de crisis sistémicas, entre otras funciones que tiene encomendadas y que realiza con gran profesionalidad y éxito.

La defensa de la seguridad energética no puede renunciar a la sostenibilidad ambiental ni a la justicia social. Estrategias de economía circular en logística y mantenimiento militar, reducción de la huella ambiental, aprovechamiento de residuos y desarrollo de infraestructuras verdes duales, civiles y militares, son ya una realidad que se deben seguir desarrollando y que favorecen tanto la eficiencia del sistema como el refuerzo de la autonomía estratégica.

Así, la integración de enfoques de transición justa, formación inclusiva y gobernanza de los procesos de cambio existentes asegura la cohesión y la resiliencia social ante transformaciones disruptivas y riesgos sociales ligados a políticas energéticas en una situación geopolítica cambiante y crítica.

Por lo que respecta a la gobernanza institucional ha de evolucionar hacia modelos cooperativos, con agencias multidisciplinares, redes de intercambio de información y sistemas de alerta temprana que permitan la coordinación eficiente entre administraciones nacionales y supranacionales[11].

Para España y la Unión Europea, el diseño e implementación de mecanismos colaborativos en inteligencia energética resulta clave para reforzar la resiliencia, prever amenazas híbridas y garantizar la seguridad transfronteriza de la infraestructura y los flujos energéticos. El modelo español y europeo avanza hacia una gobernanza multinivel con observatorios nacionales, redes europeas de inteligencia, plataformas privadas y alianzas OTAN-UE para defensa energética[12]. Además, el desarrollo de centros de pensamiento, programas avanzados, simulacros conjuntos y ejercicios de prospectiva profesionaliza y diversifica la cultura estratégica nacional y europea.

En particular, España destaca en proyectos de cooperación y formación avanzada, liderando iniciativas en hidrógeno verde, digitalización de redes, entrenamiento intersectorial y exportando modelos de protección y resiliencia en sus áreas de influencia, como el Mediterráneo.

## 7. Acciones y propuestas estratégicas para España y la UE

España, por su excepcional posición geoestratégica y su dependencia energética externa, debe priorizar una estrategia ambiciosa, resolutiva y transparente en materia de inteligencia económica y seguridad energética.

11. Véase REAL INSTITUTO ELCANO, *Inteligencia económica..., op. cit.*

12. Véase Poza Cano, D., *Energía..., op. cit.*, 2024; DEPARTAMENTO DE SEGURIDAD NACIONAL, *Informe Anual..., op. cit.*

En ese sentido deben tenerse en cuenta diferentes líneas de actuación que incluyan los siguientes aspectos fundamentales:

a) El fortalecimiento del sistema nacional de inteligencia energética, incluyendo observatorios especializados, una red nacional de analistas y realizando una integración real y eficiente de las capacidades en defensa, industria y academia.

b) El desarrollo de protocolos de respuesta ante crisis energéticas, ciber-amenazas y disrupciones del suministro, tanto de productos energéticos, como de minerales críticos y estratégicos.

c) La realización de fuertes inversiones en tecnologías de almacenamiento, redes inteligentes, I+D+i energética, ciberseguridad, inteligencia artificial, hidrógeno limpio e I+D en materiales críticos, que le permitan afrontar con éxito la nueva realidad energética.

d) La creación de reservas estratégicas dinámicas y sistemas de alerta temprana automatizados, que permita anticiparse ante posibles disrupciones.

e) La integración de la sostenibilidad y la transición justa como ejes estructurales en todas las políticas públicas y de seguridad energética.

f) El fomento de la cooperación internacional en reservas estratégicas, infraestructuras críticas y gobernanza supranacional, especialmente en el ámbito de la Unión Europea y el Mediterráneo, aprovechando su excelente situación geoestratégica.

g) La sensibilización y educación ciudadana en cultura de defensa energética, generando una percepción colectiva sobre la importancia estratégica del sector y la vulnerabilidad nacional y la formación continua de profesionales en cultura de defensa y gestión de riesgos.

h) La promoción del liderazgo español en proyectos de transición y autonomía energética europeos, como son el hidrógeno verde, las interconexiones eléctricas, la digitalización de redes y los *clusters* de innovación.

i) El desarrollo de escenarios a 2035-2050 para anticipar tendencias disruptivas, consolidando a España y la UE como *hubs* seguros, eficientes e innovadores.

Por su parte, a nivel europeo, urge la articulación de una inteligencia energética común de todos los países de la UE, la coordinación de reservas estratégicas y la protección compartida de infraestructuras críticas transfronterizas, que permitan aseguran su independencia y seguridad energética.

## 8. Perspectivas futuras y conclusiones

El futuro de la seguridad energética y la defensa nacional debe ser necesariamente prospectivo, multidimensional e interoperable, para asegurar el funcionamiento de nuestro sistema energético y el desarrollo económico.

Por su parte, la inteligencia económica aplicada al sector energético y a la cultura de defensa es un instrumento central para garantizar la autonomía, la competitividad y la resiliencia de los Estados en el siglo XXI. Su consolidación debe ser una prioridad en la agenda política, institucional y empresarial, con inversiones sostenidas en capacidades analíticas, tecnológicas y humanas.

a) Con todo se pueden considerar una serie de escenarios globales que definirán el futuro del sector en los próximos años y que incluyen, entre otros aspectos, los siguientes:

b) La intensificación de la competencia internacional por recursos energéticos y tecnológicos.

c) La evolución de amenazas híbridas y ciberamenazas a cadenas de suministro e infraestructuras críticas energéticas.

d) El incremento de la sofisticación y dificultad del análisis mediante inteligencia artificial y Big Data.

e) La creciente importancia de la formación, cooperación internacional técnica y gobernanza supranacional.

f) El reforzamiento del papel geopolítico de España como nodo estratégico energético en Europa y el Mediterráneo.

# BIBLIOGRAFÍA

**Bernaldo, M. O.**, *Transición energética sostenible. Una transición inteligente hacia un modelo energético sostenible para España en 2050*, 2021.

**Cárdenas Escorcia, Y.**, *Eficiencia Energética: Búsqueda de la Gestión inteligente de la energía*, 2024.

**Chacón Rueda, A. M.**, Análisis del sector energético y el crecimiento de las energías renovables, 2021.

**FAEN**, *Inteligencia Artificial, Datos y Energía*, 2024.

**DEPARTAMENTO DE SEGURIDAD NACIONAL**, *Informe Anual de Seguridad Nacional*, 2024.

**Fernández Carrillo, A.**, *Aplicaciones de la inteligencia artificial a las energías renovables*, 2024

**Huaquipaco Encinas, S.**, **Beltrán Castañón, N.**, **Cruz de la Cruz, J. E.**, *Inteligencia artificial y energías renovables. Un futuro energético inteligente y sostenible. Colegio de Ingenieros del Perú*, 2024.

**IEEE**, *La inteligencia económica en un mundo globalizado. Cuadernos de Estrategia*, núm. 162, 2021

**INSTITUTE FOR GLOBAL CHANGE**, *Greening AI: A Policy Agenda for the Artificial Intelligence and Energy Revolutions*, 2024.

**Izquierdo, J.**, *Seguridad energética y cohesión social,* En Barataria, 2023, pp. 445-455.

**KPMG**, *La IA y la transición energética: ¿aliadas estratégicas?*, 2024.

**Lara, F. J.**, Análisis del sector de las energías renovables en España, 2020.

**Poza Cano, D.**, *Energía y geoestrategia.* Ministerio de Defensa, 2024.

**Reglero, J.**, La importancia del sector energético en la economía, 2022.

**RH ASESORES IMPROVING**, *Inteligencia Energética (recurso divulgativo)*, 2025.

**REAL INSTITUTO ELCANO**, *Inteligencia económica como vector internacional de seguridad*. Documento de Trabajo, 2022.

**VARIOS AUTORES**, *Inteligencia artificial aplicada a los sistemas energéticos.* Editorial UAO, 2022.

# LA ACTUACIÓN DE LOS SERVICIOS DE INTELIGENCIA EN LA PROTECCIÓN DEL MEDIOAMBIENTE

**Alejandra Moreno García**

*Presidenta de la Asociación de Jóvenes en Inteligencia, Defensa y Seguridad (INDESEC)*
*Abogada en Derecho público y regulatorio*

## 1. Introducción

La creciente preocupación por el deterioro del medio ambiente ha llevado a la Unión Europea (UE) a consolidar un marco normativo amplio en materia medioambiental, cuyo objetivo es reforzar la protección del entorno natural, prevenir el deterioro ecológico y promover un desarrollo sostenible. Sin embargo, en la práctica, el cumplimiento de toda esta envergadura normativa resulta muy costoso para las empresas tanto a nivel administrativo como económico, lo que ha contribuido al aumento de prácticas ilegales vinculadas al crimen ecológico o medioambiental.

Este tipo delictivo ha emergido en los últimos años como una de las actividades ilícitas más lucrativas y de rápido crecimiento. Entre sus actividades se encuentran, entre otras: el tráfico ilegal de residuos, la caza y venta ilícita de especies protegidas, la explotación no autorizada de recursos naturales o la contaminación industrial. Se trata de un fenómeno silencioso y de baja visibilidad que está estrechamente vinculado a redes de crimen organizado y flujos financieros ilícitos, lo que dificulta su detección, persecución y sanción.

En este contexto, la inteligencia —entendida como el «*producto resultante de la recolección, evaluación, análisis, integración e interpretación de toda la información disponible, y que es inmediatamente o potencialmente significativa para la planificación y las operaciones*»[1]— se presenta como una herramienta estratégica con gran potencial para reforzar la seguridad ecológica. Sin embargo, su aplicación en el ámbito medioambiental continúa siendo limitada y poco sistematizada.

1. CENTRO CRIPTOLÓGICO NACIONAL, CCN, *Guía de Seguridad CCN-STIC-425: Ciclo de inteligencia y análisis de intrusiones*, Centro Criptológico Nacional, 2015, pág. 5.

El objetivo general de este trabajo es analizar cuál es el papel de la inteligencia en la lucha contra el crimen medioambiental en el contexto europeo. A partir de este, se derivan las siguientes preguntas específicas: ¿Cómo está estructurado el marco estratégico y operativo de la inteligencia ambiental en la Unión Europea?; ¿Cuáles son los principales factores que explican la criminalidad medioambiental en la Unión Europea y cuáles son sus impactos sociales y económicos?; ¿Qué desafíos enfrentan los actores públicos y privados en la prevención, detección y persecución del crimen medioambiental?; y finalmente, ¿Qué elementos debería incluir un modelo estratégico de inteligencia ambiental que fortalezca la prevención y la cooperación institucional en este ámbito? Estas preguntas permiten delimitar el campo de estudio y establecer una base sólida para el desarrollo del análisis.

La presente investigación adopta una metodología cualitativa de carácter exploratorio y analítico, basada principalmente en el análisis documental y normativo. Esta elección se justifica por la naturaleza del objeto de estudio, que implica el examen de marcos legales, estratégicos y operativos relacionados con la inteligencia ambiental y el crimen medioambiental en el contexto europeo. A través del estudio de fuentes secundarias —tales como legislación comunitaria, informes de organismos internacionales, estrategias institucionales, literatura académica especializada y casos relevantes— se busca identificar patrones, desafíos y oportunidades en la aplicación de la inteligencia al ámbito ambiental. Esta metodología permite comprender en profundidad los procesos y actores implicados, así como proponer modelos estratégicos fundamentados en evidencia y en buenas prácticas ya existentes.

# 2. El crimen medioambiental en la Unión Europea

## 2.1. Conceptualización y tipologías

La Directiva (UE) 2014/1203 del Parlamento Europeo y del Consejo, de 11 de abril de 2024, relativa a la protección del medio ambiente mediante el Derecho penal y por la que se sustituyen las Directivas 2008/99/CE y 2009/123/CE[2] define la delincuencia medioambiental como el conjunto de conductas intencionadas, o cometidas al menos, por imprudencia grave que vulneren el Derecho medioambiental de la Unión Europea.

En su artículo tercero, indica que, «*los Estados miembros garantizarán que las siguientes conductas constituyan delito cuando sean ilícitas e intencionadas*»:

2. PARLAMENTO EUROPEO Y CONSEJO DE LA UNIÓN EUROPEA, *Directiva (UE) 2024/1203 del Parlamento Europeo y del Consejo, de 11 de abril de 2024, relativa a la protección del medio ambiente mediante el Derecho penal y por la que se sustituyen las Directivas 2008/99/CE y 2009/123/CE*, Diario Oficial de la Unión Europea, L, 2024/1203, 2024.

a) Vertidos o emisiones contaminantes que causen o puedan causar daños graves a personas o al medio ambiente.
b) Comercialización de productos prohibidos que generen vertidos o emisiones peligrosas.
c) Uso, fabricación o venta de sustancias peligrosas restringidas o prohibidas por la normativa europea.
d) Manipulación ilegal de mercurio y productos relacionados.
e) Ejecución de proyectos sin autorización ambiental, con daños potenciales al medio.
f) Gestión ilegal de residuos, especialmente peligrosos o en cantidades significativas.
g) Traslado ilícito de residuos, incluso en operaciones vinculadas.
h) Reciclaje de buques incumpliendo la normativa ambiental.
i) Descargas contaminantes desde buques fuera de las excepciones legales.
j) Operación o cierre de instalaciones peligrosas, con riesgo ambiental o humano.
k) Construcción o desmantelamiento de instalaciones petroleras o similares de forma ilícita.
l) Manejo indebido de material radiactivo, con riesgo para personas o el entorno.
m) Extracción ilegal de aguas que degrade el estado ecológico del recurso.
n) Captura o comercio de especies protegidas, salvo cantidades insignificantes.
o) Tráfico ilegal de especies silvestres o sus derivados.
p) Comercio de productos cuya importación o exportación está prohibida por impacto ambiental.
q) Deterioro de hábitats protegidos o alteración de especies en zonas protegidas.
r) Introducción o manejo de especies invasoras, infringiendo restricciones o condiciones.
s) Uso de sustancias que agotan la capa de ozono, o de productos que las contengan.
t) Uso de gases fluorados de efecto invernadero, o de aparatos que los utilicen, sin cumplir la normativa.

Se observa así como la delincuencia medioambiental abarca una amplia gama de conductas ilegales que provocan daños significativos a los eco-

sistemas. Además, a diferencia de otros delitos, este tipo de delincuencia se caracteriza por su baja visibilidad, su complejidad técnica y su estrecha relación con redes de crimen organizado y corrupción. Esto facilita que el *iter criminis* se desarrolle frecuentemente a nivel transnacional, aprovechando vacíos normativos y desigualdades en la aplicación de la ley entre países.

## 2.2. Factores de crecimiento del crimen medioambiental y motivaciones

El crecimiento sostenido del crimen medioambiental responde a una combinación compleja de factores estructurales, sociales y culturales que dificultan su prevención y persecución. De acuerdo con el estudio sobre el origen y las motivaciones de la criminalidad ambiental de SEO/BirdLife y *Sociedade Portuguesa para o Estudo das Aves*[3] existen una serie de motivaciones recurrentes que explican la persistencia y expansión de estas prácticas ilícitas entre ellas destacan las siguientes:

a) La motivación económica constituye el principal motor de estos delitos. La obtención de beneficios rápidos y elevados, con un riesgo legal relativamente bajo en comparación con otras actividades ilícitas, hace que el tráfico de residuos, de especies protegidas o de recursos naturales resulte extremadamente atractivo para redes criminales. En contextos rurales o empobrecidos, estas prácticas también pueden estar relacionadas con la subsistencia directa, como sucede con la caza ilegal o la quema de terrenos para el pastoreo.

b) La corrupción institucional también refuerza estas dinámicas, facilitando la penetración de organizaciones delictivas en procesos legales como el comercio internacional, los controles aduaneros o los sistemas de licencias. La permisividad o complicidad de funcionarios públicos permite que estas actividades se desarrollen con mayor impunidad.

c) En algunos territorios, especialmente aquellos afectados por conflictos armados o inseguridad crónica, el crimen ambiental se convierte en una fuente adicional de financiación para grupos armados o insurgentes. La debilidad del Estado, la escasa presencia institucional y el acceso a recursos naturales valiosos generan un entorno favorable para la extracción ilegal, mientras que el comercio clandestino de fauna o flora sirve para sostener financieramente a estos actores.

3. SEO/BIRDLIFE Y SOCIEDADE PORTUGUESA PARA O ESTUDO DAS AVES, *Estudio sobre el origen y las motivaciones de la criminalidad ambiental*, Sección 1.1, SEO BirdLife, Madrid y Lisboa, 2020.

d) Otra dimensión importante está relacionada con factores culturales y creencias tradicionales. En muchas regiones, la demanda de partes animales utilizadas en prácticas *pseudoterapéuticas*, rituales o como productos de prestigio social —como los cuernos de rinoceronte, el marfil o ciertas maderas— responde a creencias arraigadas y difíciles de erradicar. En algunos casos, se han documentado incluso vínculos entre incendios provocados y rituales esotéricos.

e) Las prácticas heredadas o tradicionales también juegan un papel relevante. Modalidades de pesca, caza o uso del fuego con fines agrícolas, aunque prohibidas, siguen siendo comunes en ciertas comunidades debido a su fuerte arraigo histórico. Estas actividades suelen estar legitimadas socialmente y percibidas como parte de la vida cotidiana o del patrimonio cultural local.

f) También existe una dimensión ligada al estatus y la exclusividad. La adquisición y consumo de productos derivados de especies protegidas o recursos naturales escasos está, en muchos casos, vinculada a contextos elitistas donde estos bienes funcionan como símbolos de poder, lujo o distinción social.

g) Por otra parte, no debe subestimarse el peso del desacuerdo social con la normativa ambiental. Algunas acciones delictivas se explican como respuestas a políticas consideradas injustas, restrictivas o contrarias a los intereses locales. Es el caso de incendios provocados como protesta, o la persecución de depredadores protegidos ante la percepción de desprotección de la ganadería o los cultivos.

h) Finalmente, un factor común a muchos de estos delitos es el desapego emocional o cultural hacia el medio ambiente, así como una limitada comprensión del impacto real de las acciones. Este distanciamiento favorece la indiferencia ante la destrucción del entorno natural y la falta de empatía con los recursos que se explotan o dañan.

En conjunto, estos factores demuestran que el crimen medioambiental no es únicamente una cuestión de legalidad, sino también de contexto social, económico y cultural.

## 2.3. Impacto ecológico, social y económico

El crimen medioambiental se ha consolidado como una de las amenazas más graves y complejas para la seguridad global. Según el Consejo de la Unión Europea[4], se trata de la tercera actividad delictiva más extendida en el mundo, solo por detrás del tráfico de drogas y la falsificación, con un ritmo de crecimiento anual estimado entre el 5 % y el 7 %. La delincuencia medioam-

4. EUROPOL, COMISIÓN EUROPEA, INTERPOL Y NACIONES UNIDAS, «*La lucha de la UE contra la delincuencia medioambiental*, EMPACT, Infografía, La Haya, 2023.

biental no solo representa una amenaza directa al entorno natural, sino que también conlleva consecuencias profundas para la salud humana, el tejido social y la economía global.

Según los datos publicados por el Consejo de la Unión Europea (2022), este tipo de criminalidad provoca un aumento significativo de los niveles de contaminación, contribuye a la degradación de la fauna silvestre y acelera la pérdida de biodiversidad. Estas alteraciones comprometen el equilibrio ecológico de regiones enteras y generan efectos acumulativos que afectan tanto a los ecosistemas como a las poblaciones humanas que dependen de ellos.

Uno de los impactos más visibles es la pérdida de especies protegidas, cuya extracción ilegal alimenta mercados internacionales lucrativos. En 2022, las autoridades europeas incautaron más de 1.000 ejemplares de flora y fauna silvestres amenazadas, incluyendo colmillos de elefante, cuernos de rinoceronte, aves exóticas y artículos elaborados con coral. Estas actividades, además de destruir hábitats, alimentan redes de tráfico que suelen operar con altos niveles de organización y violencia.

También se ha detectado un elevado volumen de tráfico ilegal de residuos y gases contaminantes. Ese mismo año se incautaron más de 334.000 toneladas de residuos, muchos de ellos enviados desde Europa hacia Asia y África, lo que convierte a la UE en una fuente clave de desechos en estas rutas delictivas. Entre los materiales incautados figuran residuos electrónicos, textiles, plásticos y papel. Además, se confiscaron casi 640.000 kg de gases fluorados, con un valor de mercado superior a los 12 millones de euros. Estos gases, al tener una capacidad de calentamiento muy superior a la del CO2, agravan los efectos del cambio climático.

La delincuencia medioambiental tiene un impacto económico significativo, con pérdidas estimadas que oscilan entre 110.000 y 281.000 millones de dólares al año. Estas cifras reflejan no solo los costes directos —como la restauración de los ecosistemas degradados o la disminución de ingresos procedentes del turismo sostenible—, sino también los efectos indirectos sobre la salud pública, la seguridad alimentaria y el comercio legal. Esta magnitud económica pone de manifiesto la capacidad de estas actividades delictivas para infiltrarse en sistemas legales y comerciales, generando graves consecuencias a nivel global.

La infografía elaborada por el Consejo de la Unión Europea recopila los esfuerzos de la UE destinados a combatir el crimen medioambiental en el marco de la plataforma EMPACT (Plataforma Europea Multidisciplinar contra las Amenazas Criminales) —una iniciativa europea de lucha contra la delincuencia organizada y grave internacional—. En ella se destaca que los vínculos entre estos delitos y las redes criminales organizadas refuerzan la urgente necesidad de abordarlos no solo como un problema ecológico, sino también como un asunto de seguridad. Solo en el año 2022, las operaciones policiales en la UE llevaron a la detención de 401 personas y a incautaciones

por un valor total de 15 millones de euros, lo que evidencia la magnitud económico-financiera de estas redes ilícitas y su capacidad para evadir la ley y corromper instituciones.

# 3. La seguridad ambiental y los servicios de inteligencia

## 3.1. Servicios de inteligencia: actores clave en la lucha contra el crimen medioambiental

La lucha contra el crimen medioambiental implica la coordinación de múltiples actores nacionales e internacionales que operan a diferentes niveles de competencia. Esta complejidad responde tanto a la naturaleza transnacional de muchos delitos medioambientales como a la diversidad de marcos jurídicos, operativos y administrativos en los que actúan las distintas instituciones implicadas.

En el ámbito europeo, Europol desempeña un papel central como agencia de apoyo a las fuerzas de seguridad nacionales, facilitando el intercambio de inteligencia, el análisis estratégico y la coordinación operativa en todo tipo de crímenes internacionales, incluyendo el crimen medioambiental[5] a través de plataformas como EMPACT. Asimismo, Eurojust, en colaboración con redes como ENPE (*European Network of Prosecutors for the Environment*), contribuye a fortalecer la cooperación judicial, la armonización interpretativa de las normas y la formación especializada de jueces y fiscales en materia ambiental[6].

A nivel técnico-operativo, destaca la red EnviCrimeNet[7], que integra a profesionales de cuerpos policiales y autoridades regulatorias medioambientales de los distintos Estados miembros. Esta red ha promovido iniciativas como el Proyecto de Inteligencia sobre Delito Medioambiental (en adelante IPEC), que ha permitido identificar patrones delictivos, debilidades estructurales y oportunidades para mejorar el intercambio de información y la respuesta coordinada.

Por su parte, las autoridades interiores incluyen:

a) unidades policiales especializadas (por ejemplo, el Servicio de Protección de la Naturaleza (SEPRONA) en España o los Carabinieri forestales en Italia);

5. MANAGEMENT BOARD OF EUROPOL, *Europol Programming Document 2025-2027*, La Haya, EUROPOL, 2024, págs. 38-39.

6. EUROPEAN NETWORK OF PROSECUTORS FOR THE ENVIRONMENT (ENPE), *LIFE-ENPE Layman's report, ENPE,* 2020, pág. 5.

7. ENVICRIMENET*, Fight against environmental crime at a strategic level through the strengthening of EnviCrimeNet. LAYMAN'S REPORT*, *LIFE + SATEC,* 2023.

b) cuerpos de aduanas y guardias fronterizos, que desempeñan funciones cruciales en la detección, inspección y persecución de infracciones ambientales.

En el plano global, instituciones como Interpol, la Oficina de Naciones Unidas contra la Droga y el Delito (ONUDD) y el Consorcio Internacional para Combatir los Delitos contra la Vida Silvestre (ICCWC) contribuyen al establecimiento de estándares internacionales, campañas de visibilizarían, intercambio de inteligencia y formación técnica.

Paralelamente, organizaciones no gubernamentales como la WWF o SEO-BirdLife, presentan denuncias, ponen en marcha actuaciones de seguimiento para aumentar la detección temprana de estos delitos y aportan valiosa evidencia mediante investigaciones y elaboración de informes en materia medioambiental[8]. Además, presionan a los gobiernos para una mayor ambición normativa y sancionadora.

En conjunto, esta arquitectura multinivel refleja la creciente comprensión de que el crimen medioambiental representa una amenaza tanto para los ecosistemas como para la gobernanza democrática. La cooperación entre estos actores, aunque a menudo se encuentra obstaculizada por barreras legales, falta de interoperabilidad de bases de datos o carencias de personal está en proceso de evolución dado que resulta esencial para generar respuestas efectivas y sostenibles.

## 3.2. La dimensión estratégica de la seguridad ambiental

En el marco de la Unión Europea, se han desarrollado iniciativas para reconocer la criminalidad medioambiental como un asunto estratégico[9]. Una de las primeras respuestas fue la creación de redes sectoriales compuestas por representantes del ámbito judicial, administrativo y policial. Estas estructuras, conocidas como *4-network*, han permitido fomentar la cooperación especializada y asesorar en materia legislativa[10].

Un hito relevante fue el IPEC[11], promovido por EnviCrimeNet y Europol, que reveló la complejidad y el carácter lucrativo de estos delitos, muchos de ellos centrados en el tráfico ilegal de residuos y especies protegidas. El informe destacó la necesidad de compartir información entre agencias, de reforzar las capacidades nacionales y de contar con marcos normativos actualizados que incluyan directivas específicas y unidades especializadas.

8. De la Bodega, D.; Cano, C.; Mínguez, E, «*El veneno en España. Evolución del envenenamiento de fauna silvestre (19922017)*», SEO/BirdLife y WWF España, Madrid, 2020.

9. EUROPOL, *Europol Environmental Statement* 2021, EUROPOL, La Haya, 2021, pág. 9-10.

10. *Ibid*., pág. 10.

11. ENVICRIMENET; EUROPOL, *Intelligence Project on Environmental Crime*, ENVICRIMENET, La Haya, 2015, págs. 1-2.

En este contexto, la seguridad ambiental se consolida como una dimensión que trasciende la protección ecológica, exigiendo una respuesta estructurada y basada en inteligencia, tanto a nivel nacional como europeo. Planes como el Plan de Acción contra el tráfico de vida silvestre han contribuido a operacionalizar estas estrategias, otorgando a organismos como Eurojust y Europol un rol clave en la articulación de políticas preventivas y de persecución del crimen medioambiental[12].

En los últimos años también se ha incluido el crimen medioambiental como una de las áreas de la plataforma EMPACT, lo que ha dado lugar a un despliegue de actividades tanto operativas como estratégicas desde el año 2018, fecha en la que además se firmó la Política Medioambiental de Europol por su Director Ejecutivo[13]. Un documento en el que se regula el desarrollo de un Sistema de Gestión Medioambiental y un mecanismo de control y se fijan objetivos organizativos para que la organización sea asimismo más sostenible reduciendo las emisiones de CO2. En el ámbito interno español, desde el año 2017, se incluye en la Estrategia de Seguridad Nacional la preservación del medio ambiente y la biodiversidad como uno de los principales ámbitos de actuación de la política nacional[14].

## 3.3. Operaciones relevantes en la lucha contra la delincuencia medioambiental

En los últimos años, las Fuerzas y Cuerpos de Seguridad (en adelante FCS) han desarrollado operaciones de alcance internacional que evidencian un compromiso creciente con la persecución del crimen medioambiental, especialmente en lo referente al tráfico ilícito de residuos. Una de las iniciativas más representativas en este campo ha sido la Operación *30 DÍAS DE ACCIÓN*, liderada por Interpol en 2017[15], que movilizó a agencias policiales, aduaneras y medioambientales de 43 países. Durante un mes de actividades coordinadas, se detectaron más de 660 infracciones relacionadas con residuos ilegales, involucrando a casi 500 personas y más de 260 empresas. El valor estimado de los residuos incautados rondó los 33 millones de dólares, destacando también la detección de aproximadamente 56.000 toneladas de residuos plásticos mal gestionados, lo que refleja la dimensión económica y ambiental de este tipo de delitos.

12. Alfaro Moreno, J. A., «*Aproximación a las consecuencias de la priorización del delito ambiental en la Unión Europea» en* Cuadernos de la Guardia Civil, Revista de Seguridad Pública, núm. 69, Dirección General de la Guardia Civil, 2023, pág. 32

13. EUROPOL, *2018. Consolidated Annual Activity Report*, EUROPOL, Bucarest, 2019, pág. 52.

14. DEPARTAMENTO DE SEGURIDAD NACIONAL, *Estrategia de Seguridad Nacional, 2017* Gobierno de España, Madrid, 2017, pág. 13.

15. INTERPOL, *Emerging Criminal Trends in the Global Plastic Waste Market since January 2018*, Interpol General Secretariat, Lyon, 2020, pág. 13.

En el marco de la cooperación internacional, destaca también la *Operación DEMETER IV*[16]*,* coordinada por la Organización Mundial de Aduanas (OMA) y promovida inicialmente por la Administración de Aduanas de China. Esta operación, se centró en frenar los movimientos transfronterizos ilegales de residuos. Participaron 75 administraciones aduaneras de distintos continentes, convirtiéndola en la mayor operación aduanera contra el tráfico ilícito de residuos hasta la fecha. Se logró intervenir más de 326.000 toneladas y cerca de 55.000 unidades de diversos residuos, entre los que destacaban escorias minerales, residuos plásticos, electrónicos, textiles, metales y neumáticos usados. Uno de los decomisos más significativos fue la interceptación de un cargamento de escoria de fundición, procedente de España, con un volumen aproximado de 180.000 toneladas.

El operativo contó con el respaldo de organizaciones como Interpol, Europol, la Convención de Basilea y la Oficina para Asia y el Pacífico del Programa de las Naciones Unidas para el Medio Ambiente, entre otros. Durante su desarrollo se emplearon técnicas avanzadas de análisis de riesgo y selección de objetivos, con el uso de plataformas seguras para la coordinación y el intercambio de Inteligencia en tiempo real. Las cifras obtenidas en ambas operaciones ponen de relieve el carácter lucrativo de estas actividades ilegales y la necesidad urgente de dotar a las FCS de recursos adecuados para enfrentarlas de forma eficaz. En conjunto, estas actuaciones demuestran que el crimen medioambiental, requiere de estrategias conjuntas, tecnología especializada y una sólida cooperación transnacional.

## 3.4. Inteligencia y retos frente a la delincuencia ambiental

De acuerdo con lo establecido en el informe de EnviCrimeNet sobre delitos contra el medio ambiente en Europa[17], la lucha contra el delito medioambiental enfrenta numerosos retos en materia de Inteligencia y cooperación institucional.

Uno de los principales obstáculos es la fragmentación entre autoridades regulatorias y FCS. Esta fragmentación dificulta la cooperación, especialmente en lo que respecta al intercambio de datos e información entre autoridades o, en el mejor de los casos, lo hacen de forma lenta e incompleta, lo que favorece respuestas poco coordinadas, incluso cuando existen intereses comunes.

A nivel operativo, las FCS enfrentan limitaciones presupuestarias que dan lugar a falta de formación y escasez de unidades especializadas, lo que

16. WORLD CUSTOMS ORGANIZATION (WCO), *Customs successfully target environmentally sensitive goods during Operation DEMETER V*, WCO, La Haya, 2019.

17. ENVICRIMENET, *Intelligence Project on Environmental Crime. Report on Environmental Crime in Europe*, ENVICRIMENET, La Haya, 2015, pág.16.

impide la generación de inteligencia estratégica para prevenir y detectar los delitos. A esto se suma que muchas autoridades supervisoras carecen de mecanismos estandarizados de denuncia o intercambio de información, lo que impide aprovechar sinergias entre organismos.

En el plano internacional ocurre algo similar: la cooperación transfronteriza es débil. La falta de redes oficiales de contacto, las diferencias legislativas entre Estados y la ausencia de sistemas comunes para el seguimiento de actividades ilícitas como el tráfico de residuos o especies protegidas, permiten a las redes criminales operar con relativa impunidad.

En el caso de la gestión de residuos —actividad señalada por Europol e Interpol como una de las áreas delictivas principales explotadas por organizaciones criminales a nivel internacional—, uno de los principales desafíos radica en fomentar un intercambio efectivo de inteligencia y en la coordinación práctica y asignación de recursos entre países. En el ámbito de la Unión Europea, no existe una coordinación adecuada, especialmente en lo que respecta al traslado de residuos, incluidos los residuos de aparatos eléctricos y electrónicos (RAEE), dado que no se dispone de sistemas electrónicos ni bases de datos comunes, tanto a nivel europeo como internacional, que permitan un seguimiento eficaz de estos movimientos.

Además, no existe un sistema europeo unificado para abordar conductas ilegales que no alcanzan el umbral penal, ni se ha establecido un enfoque multinacional y multiagencial para combatir este tipo de delincuencia ambiental, ni tampoco una entidad oficial de la UE dedicada a esta función. Por consiguiente, la capacidad de adaptación del crimen organizado, junto con su aprovechamiento del entorno digital y la experiencia acumulada en otros tipos de tráfico ilícito, les proporciona una ventaja significativa frente a las estructuras estatales, que suelen estar fragmentadas. A esta situación se suman la insuficiencia de recursos, la baja prioridad política y judicial otorgada al problema, así como las dificultades estructurales ya mencionadas, factores que contribuyen a que muchos casos nunca sean objeto de una investigación profunda.

El último Documento de programación de Europol para los años 2025-2027, aprobado por el Consejo de Administración de Europol el 10 de diciembre de 2024 señala que, uno de los objetivos de Europol es prestar apoyo a las investigaciones de los Estados miembros de la UE sobre delitos ambientales. Entre estos objetivos destacan algunos como[18]:

a) Realizar el tratamiento de datos, análisis de inteligencia criminal y prestar apoyo a los Estados miembros con capacidades y conocimientos operativos, incluido el apoyo in situ. Compartir la lista de Europol de recursos técnicos disponibles (como laboratorios acre-

18. MANAGEMENT BOARD OF EUROPOL, *Europol Programming Document 2025-2027,* EUROPOL, La Haya, 2024, págs 68-69.

ditados, empresas de muestreo, etc.) en la UE que puedan utilizarse para responder a necesidades operativas concretas en investigaciones de delitos medioambientales por parte de los Estados miembros.

b) Apoyar las investigaciones de los Estados miembros en delitos transfronterizos relacionados con residuos y contaminación, así como en casos de infiltración de redes delictivas en estructuras empresariales legales correspondientes.

c) Centrarse en el tráfico de gases fluorados de efecto invernadero (gases F) y sustancias que agotan la capa de ozono, en particular en aquellos casos que incluyan la infiltración de estructuras empresariales legales y actividades facilitadas por internet.

d) Enfocarse en la gestión ilícita de residuos de aparatos eléctricos y electrónicos, especialmente en la exportación a terceros países.

e) Impulsar asociaciones para la lucha contra la delincuencia medioambiental mediante alianzas específicas, incluidas partes privadas relevantes, a fin de fortalecer la cooperación operativa dirigida, abordar lagunas en inteligencia, compartir conocimientos, fomentar la innovación, desarrollar capacidades y resolver conjuntamente los desafíos existentes.

## 4. Herramientas para la inteligencia ambiental

La inteligencia ambiental se nutre principalmente de información obtenida mediante herramientas de inteligencia geoespacial (GEOINT), que integran imágenes, datos y productos técnicos derivados del análisis espacial, espectral y temporal del territorio. La *geointeligencia*, según la reseña escrita por Caddell, se define como[19]: *«un campo complejo que integra diversas disciplinas como la inteligencia de imágenes, cartografía, navegación precisa, ciencias de la información geográfica, geodesia y visualización gráfica. Aunque su definición puede variar dependiendo del contexto, en términos generales, GEOINT se refiere al análisis y la interpretación de datos espaciales y temporales para apoyar la toma de decisiones en el ámbito de la inteligencia. Esta disciplina combina información proveniente de sensores remotos, sistemas de información geográfica y otras fuentes para proporcionar una comprensión profunda del entorno físico y humano. En el contexto de la comunidad de inteligencia, GEOINT se asocia especialmente con el uso de datos clasificados y no clasificados derivados de imágenes satelitales y otros medios de vigilancia espacial, que son analizados para obtener información relevante sobre actividades y patrones en un espacio geográfico».*

19. Caddell, J. W., «*Geospatial Intelligence: Origins and Evolution*, Studies in Intelligence», vol. 65, núm. 1, 2021, págs. 39-41.

Esta herramienta —en constante evolución— resulta estratégica en el ámbito de la Inteligencia ambiental. Gracias a ella, los servicios encargados del cumplimiento de la normativa ecológica pueden detectar de forma temprana actividades ilícitas como la deforestación ilegal, el vertido de residuos o el uso no autorizado del suelo, así como reunir pruebas técnicas fiables.

El crecimiento del crimen ambiental ha ido de la mano con la necesidad de herramientas más sofisticadas que respondan a los retos ambientales contemporáneos, situando a la inteligencia geoespacial en el centro de las estrategias de inteligencia ante delitos ambientales.

## 4.1. Proyecto EMERITUS

El proyecto europeo EMERITUS[20] constituye un ejemplo destacado en este ámbito. Su objetivo principal es diseñar un protocolo operativo que permita una investigación más eficaz de los delitos ecológicos, integrando tecnologías emergentes como drones, sensores virtuales, imágenes satelitales y plataformas de análisis de datos espaciales. Esta iniciativa reúne a autoridades policiales y de control fronterizo de cinco países, junto con expertos en seguridad, formación y desarrollo tecnológico.

Una de las principales aportaciones del proyecto es la creación de una plataforma de *geointeligencia* capaz de consolidar información procedente de diversas autoridades para ofrecer una visión completa y contextualizada a quienes toman decisiones operativas. Asimismo, se contempla un programa de formación práctico y teórico para capacitar a los usuarios finales en el uso efectivo de esta herramienta, mediante simulaciones basadas en casos reales y entornos complejos.

El desarrollo y validación de esta tecnología no solo busca mejorar las capacidades de respuesta nacional y transfronteriza frente al crimen medioambiental, sino también proporcionar recomendaciones basadas en evidencias a los responsables políticos, con el fin de fortalecer el marco normativo y operativo en materia de protección ambiental.

## 4.2. Proyecto GIEDA: inteligencia geoespacial para la evaluación de daños ambientales

El proyecto GIEDA (*Geospatial Intelligence for Environmental Damage Assessment*), promovido por la Red de la Unión Europea para Aplicación y Cumplimiento de la Legislación Ambiental (Red IMPEL), tiene como objetivo reforzar la capacidad de las autoridades ambientales y judiciales para detec-

20. CORDIS SERVICES, *Environmental crimes' intelligence and investigation protocol based on multiple data sources*, *EMERITUS*, EUROPEAN COMISSION, Luxemburgo, 2022.

tar y demostrar daños medioambientales mediante herramientas de observación de la Tierra[21].

Esta iniciativa, activa entre 2023 y 2024, recopila casos reales en los que tecnologías como satélites, drones y análisis geoestadísticos han sido clave para identificar infracciones como vertidos ilegales, actividades no autorizadas en espacios protegidos o deforestación. El valor añadido de este proyecto radica en su enfoque integral: no solo se emplea geotecnología para vigilancia preventiva, sino también para reconstruir a posteriori eventos contaminantes, determinando dimensiones afectadas, volúmenes de residuos o el periodo en el que se produjeron los daños. La precisión de estos análisis permite que sean utilizados como prueba en procedimientos judiciales o administrativos, siempre cumpliendo con requisitos de calidad y trazabilidad técnica.

Además, GIEDA impulsa el intercambio de buenas prácticas entre agencias europeas y busca sensibilizar a operadores jurídicos sobre el potencial de estas tecnologías para fundamentar acciones legales en materia medioambiental.

## 5. Propuesta de un modelo estratégico para la inteligencia ambiental en la Unión Europea

La creciente gravedad y sofisticación de los delitos medioambientales demandan un enfoque estratégico que combine una prevención eficaz con una cooperación institucional robusta y coordinada. En este contexto, la inteligencia ambiental emerge como esencial para anticipar, detectar y responder a estas amenazas, permitiendo un análisis profundo y un intercambio ágil de información entre las distintas instituciones.

Ante este panorama, diversos informes recomiendan avanzar en la creación de plataformas interinstitucionales, fortalecer la cooperación jurídica entre Estados, dotar de medios a las unidades especializadas y generar campañas de concienciación que eleven la percepción social y judicial sobre la gravedad real de estos delitos. Sin estos pasos, la criminalidad medioambiental continuará representando una amenaza creciente, con altas ganancias para los infractores y escasos riesgos de ser sancionados.

A continuación, se plantea una propuesta de modelo estratégico de inteligencia ambiental, plenamente integrado en las políticas europeas de seguridad y sostenibilidad, y alineado con los objetivos del Pacto Verde Europeo[22]. Esta propuesta refleja el papel clave de la inteligencia en la prevención y mitigación de los daños ecológicos, considera las dificultades en la obtención de

21. Filipponi, F., Calcagni, L., Bellingeri, D., «*IMPEL Geospatial Intelligence for Environmental Damage Assessment (GIEDA) Project*», ESA-ESRIN, Frascati, 2024.

22. COMISIÓN EUROPEA, *El Pacto Verde Europeo*, EUR-Lex, Bruselas, 2019.

información y permite la participación de todos los actores de la sociedad en la lucha contra el crimen ambiental. Se propone la creación de una plataforma digital basada en Inteligencia Artificial (en adelante IA) que clasifique y priorice automáticamente las alertas ambientales, identificando patrones anómalos y niveles de riesgo para actuar con rapidez y precisión.

Esta Plataforma Integrada de Inteligencia Ambiental (en adelante PIIA), debería estar sustentada en la nube y disponer de acceso móvil (aplicación propia), a fin de facilitar la colaboración entre agentes, técnicos y decisores. PIIA debería incorporar módulos de visualización avanzada, como mapas interactivos y realidad aumentada para operaciones de campo, y herramientas forenses digitales para la generación de informes con validez jurídica. Además, PIIA debería disponer de distintas fórmulas de acceso, de manera que en función del sujeto que acceda a la misma este pueda tener límites de acceso a determinada información.

De esta manera, se podría contemplar la integración de actores no estatales, como oenegés y la ciudadanía, a través de canales seguros por medio de una aplicación móvil que permita que estos sujetos alimenten la red con información de campo y contribuyan a la detección temprana de posibles ilícitos ambientales. De esta forma, se podría ampliar la riqueza de la inteligencia ambiental a través de la fusión de fuentes heterogéneas que permitan proporcionar información por medio de: IMINT, inteligencia de imágenes; SIGINT, inteligencia de señales; o HUMINT, inteligencia de fuentes humanas.

La propia IA de PIIA gestionaría todos los datos para filtrar falsas alarmas y priorizar incidencias reales, permitiendo a su vez la anticipación de puntos críticos de riesgo y el diseño de estrategias preventivas efectivas. Por lo que respecta a la coordinación dinámica y multinivel entre los distintos actores sería necesario mejorar la capacitación de los operadores jurídicos, fiscales, agentes de inspección y cuerpos policiales especializados, a través de programas formativos que aborden el uso de herramientas tecnológicas de inteligencia ambiental y los aspectos legales vinculados.

Otro de los aspectos fundamentales del modelo estratégico es la asignación de recursos técnicos adecuados para que las unidades especializadas puedan aplicar técnicas avanzadas como el uso de drones, análisis de big data, inteligencia artificial y servicios de observación satelital. Esta inversión permitirá mejorar la precisión en la recolección y análisis de evidencias, fundamentales para la investigación y el enjuiciamiento.

Promover campañas educativas y de sensibilización dirigidas principalmente a la sociedad civil, con el objetivo de visibilizar la gravedad y el impacto real de los delitos ambientales, incentivando la denuncia y facilitando el acceso a información de valor a las FCS.

Finalmente, este modelo debe estar alineado con los principales marcos estratégicos de la Unión Europea, como el Pacto Verde Europeo y la Estrategia de Biodiversidad 2030, garantizando que la inteligencia ambiental contri-

buya no solo a la seguridad jurídica y ambiental, sino también a la protección y gestión sostenible de los recursos naturales.

## 6. Conclusiones

El presente trabajo ha permitido evidenciar la creciente relevancia del crimen medioambiental en el contexto de la Unión Europea, no solo por su impacto ecológico directo, sino también por sus profundas implicaciones sociales, económicas y de seguridad. A través de un análisis detallado, se ha observado cómo estas actividades ilícitas han evolucionado en complejidad, aprovechando vacíos legales, falta de coordinación internacional y debilidades institucionales que le permiten proliferar. En este marco, se destaca la necesidad de incorporar la dimensión ambiental dentro de las prioridades estratégicas de seguridad, reconociendo que la protección del entorno natural no puede desligarse de la estabilidad y el bienestar de las sociedades.

En este contexto, los servicios de inteligencia emergen como actores clave, no solo en la detección y prevención de delitos, sino también en la anticipación de amenazas futuras mediante el uso de tecnologías avanzadas y enfoques multidisciplinarios. Herramientas como los proyectos EMERITUS y GIEDA demuestra el potencial de la inteligencia aplicada al ámbito ambiental, especialmente en lo relativo al análisis geoespacial, la evaluación de daños y la elaboración de escenarios de riesgo. Asimismo, la propuesta de una plataforma integrada de inteligencia ambiental para la Unión Europea se plantea como un modelo estratégico viable, que permitiría mejorar la cooperación entre Estados miembros, optimizar recursos y reforzar la resiliencia institucional frente a los desafíos medioambientales.

Desde una perspectiva crítica, este estudio ha permitido cuestionar no solo la eficacia de las respuestas actuales frente a los delitos contra el medioambiente, sino también la limitada integración de los sistemas de inteligencia en esta lucha. Si bien existen avances y herramientas prometedoras, como los proyectos EMERITUS y GIEDA, aún persisten importantes desafíos estructurales, políticos y operativos que obstaculizan una acción verdaderamente coordinada y preventiva.

En definitiva, para transformar las estructuras actuales y avanzar hacia un modelo más eficaz de protección ambiental que garantice la sostenibilidad del desarrollo europeo y preserve la seguridad del entorno para las generaciones futura es necesario enfrentar el crimen medioambiental desde un enfoque integral, basado en la cooperación transnacional, el fortalecimiento de capacidades técnicas y humanas, y la consolidación de una cultura de Inteligencia ambiental entendida no como un recurso accesorio, sino como un componente central en la formulación de políticas ambientales sostenibles y en la defensa de los intereses estratégicos de la Unión Europea en materia ecológica.

# BIBLIOGRAFÍA

**Alfaro Moreno, J. A.**, «*Aproximación a las consecuencias de la priorización del delito ambiental en la Unión Europea» en* Cuadernos de la Guardia Civil, Revista de Seguridad Pública, núm. 69, Dirección General de la Guardia Civil, 2023.

**CENTRO CRIPTOLÓGICO NACIONAL**, **CCN**, *Guía de Seguridad CCN-STIC-425: Ciclo de inteligencia y análisis de intrusiones*, Centro Criptológico Nacional, 2015.

**COMISIÓN EUROPEA**, *El Pacto Verde Europeo*, EUR-Lex, Bruselas, 2019.

**Caddell, J. W.**, «*Geospatial Intelligence: Origins and Evolution*, Studies in Intelligence», vol. 65, núm. 1, 2021.

**CORDIS SERVICES**, *Environmental crimes' intelligence and investigation protocol based on multiple data sources*, *EMERITUS*, EUROPEAN COMISSION, Luxemburgo, 2022.

**De la Bodega, D.**; **Cano, C.**; **Mínguez, E.**, «*El veneno en España. Evolución del envenenamiento de fauna silvestre (19922017)»*, SEO/BirdLife y WWF España, Madrid, 2020.

**DEPARTAMENTO DE SEGURIDAD NACIONAL**, *Estrategia de Seguridad Nacional, 2017* Gobierno de España, Madrid, 2017.

**EUROPEAN NETWORK OF PROSECUTORS FOR THE ENVIRONMENT** (ENPE), *LIFE-ENPE Layman's report, ENPE,* 2020.

**EUROPOL**, *Europol Environmental Statement* 2021, EUROPOL, La Haya, 2021.

**EUROPOL**, *Europol Environmental Statement 2021*, EUROPOL, La Haya, 2021.

**ENVICRIMENET**; **EUROPOL**, *Intelligence Project on Environmental Crime*, ENVICRIMENET, La Haya, 2015.

**ENVICRIMENET**, *Fight against environmental crime at a strategic level through the strengthening of EnviCrimeNet. LAYMAN'S REPORT*, *LIFE + SATEC,* 2023.

**EUROPOL**, *2018. Consolidated Annual Activity Report*, EUROPOL, Bucarest, 2019.

**EUROPOL, COMISIÓN EUROPEA, INTERPOL Y NACIONES UNIDAS**, «*La lucha de la UE contra la delincuencia medioambiental*, EMPACT, Infografía, La Haya, 2023.

**Filipponi, F.**, **Calcagni, L.**, **Bellingeri, D.**, «*IMPEL Geospatial Intelligence for Environmental Damage Assessment (GIEDA) Project*», ESA-ESRIN, Frascati, 2024.

**INTERPOL**, *Emerging Criminal Trends in the Global Plastic Waste Market since January 2018*, Interpol General Secretariat, Lyon, 2020.

**MANAGEMENT BOARD OF EUROPOL**, *Europol Programming Document 2025-2027*, La Haya, EUROPOL, 2024.

**PARLAMENTO EUROPEO Y CONSEJO DE LA UNIÓN EUROPEA**, *Directiva (UE) 2024/1203 del Parlamento Europeo y del Consejo, de 11 de abril de 2024, relativa a la protección del medio ambiente mediante el Derecho penal y por la que se sustituyen las Directivas 2008/99/CE y 2009/123/CE*, Diario Oficial de la Unión Europea, L, 2024/1203, 2024.

**SEO/BIRDLIFE Y SOCIEDADE PORTUGUESA PARA O ESTUDO DAS AVES**, *Estudio sobre el origen y las motivaciones de la criminalidad ambiental*, Sección 1.1, SEO BirdLife, Madrid y Lisboa, 2020.

**WORLD CUSTOMS ORGANIZATION (WCO)**, *Customs successfully target environmentally sensitive goods during Operation DEMETER V*, WCO, La Haya, 2019.

# LA RADICALIZACIÓN EN PRISIONES COMO DESAFÍO PARA LOS SERVICIOS DE INTELIGENCIA

**Susana Berrocal Díaz**

*Profesora Doctora de la Universidad Europea de Valencia*

## 1. Introducción

La radicalización yihadista es un fenómeno de por sí complejo y creciente. Supone una amenaza real a la seguridad pública debiendo ser entendida como un proceso dinámico y complicado de gestionar y no como un evento único[1]. Cuando esta amenaza proviene de las prisiones, el fenómeno es aún más preocupante. La Institución Penitenciaria, que forma parte de la estructura del control social formal, tiene como fin primordial la reeducación y la reinserción de los sentenciados a penas y medidas penales privativas de libertad, así como la retención y custodia de detenidos, presos y penados.

Las prisiones, por sus propias características físicas, estructurales y también sociales, se convierten en lugares propicios para la comisión de nuevos ilícitos, pero también para la propagación de las ideas que sostienen el extremismo violento de corte yihadista. Factores como la vulnerabilidad emocional, el sentimiento de exclusión, la necesidad de pertenencia o identidad, las condiciones de hacinamiento en algunos centros penitenciarios, la violencia y la falta de recursos de reinserción así como otros muchos factores, facilitan la captación de internos por parte de individuos radicalizados que difunden su ideología violenta. Los centros penitenciarios toman el control de los sujetos que en ellos conviven bajo un régimen de vida ordenada y tienen la responsabilidad de su reeducación y reinserción, sin embargo, ¿cómo trabajar con un interno que, amparado en su supuesta religión, lanza mensajes que radicalizan a otros? ¿es suficiente con la dispersión en los casos de radicalización?, ¿es posible la reeducación y reinserción de un sujeto radicalizado?, ¿afecta a la seguridad nacional estas situaciones?, ¿es posible la intervención de los esta-

1. Borum, R., *Radicalization into violent extremism I: A review of social science theories*, Journal of Strategic Security, 4(4), 2011, págs. 7-36.

tutos de control social formal en estos casos? Son muchas las preguntas que se plantean en este contexto y no tantas las respuestas, pero lo que sí podemos dar por cierto es que la radicalización en los entornos penitenciarios es una problemática compleja que necesita de unas políticas púbicas de prevención adecuadas y coordinadas para hacer frente a la situación pero también necesita de una vigilancia constante que prevenga que, una vez cumplida condena, un sujeto excarcelado sin las condiciones de reeducación y reinserción óptimas, pueda convertirse en el sujeto activo de un delito de terrorismo.

En el caso español, la amenaza ha sido particularmente visible en el marco del extremismo de motivación religiosa, en especial el yihadismo, aunque no se limita a él. La confluencia de los factores expuestos en este mismo punto, evolucionan en ocasiones hacia la asunción de doctrinas legitimadoras de la violencia. Tal y como advierte la Oficina de las Naciones Unidas contra la Droga y el Delito, «los establecimientos penitenciarios pueden constituir un caldo de cultivo para el extremismo violento si no se implementan estrategias de gestión adecuadas»[2].

En este complejo escenario, puede entenderse que los servicios de inteligencia desempeñan un papel esencial. La inteligencia en el entorno penitenciario y en coordinación con la inteligencia policial y estratégica, puede ser la herramienta clave para anticipar, detectar y neutralizar amenazas antes de que se materialicen. El intercambio constante de información entre niveles tácticos y estratégicos permitirá integrar los datos obtenidos intramuros en un ciclo de inteligencia que sirva de base para la adopción de decisiones de seguridad a escala nacional e internacional, en el caso de la radicalización violenta especialmente. Esta interrelación entre el ámbito penitenciario y los servicios de inteligencia constituye el núcleo de análisis del presente trabajo entendiendo que la vinculación entre radicalización en prisión y trabajo de inteligencia exige un enfoque interdisciplinar que combine la Criminología, el Derecho, la Psicología Social y los estudios de seguridad y defensa.

## 2. Análisis de la problemática: la realidad de la radicalización yihadista en prisiones

En palabras de Lobato y García-Coll, la radicalización supone un proceso de extremismo sea o no este violento.[3] Se trata de un procedimiento por el cual una persona, o un grupo de ellas, adopta ideas o creencias que posteriormente pueden convertirse en conductas físicas en las que se justifica el

2. OFICINA DE LAS NACIONES UNIDAS CONTRA LA DROGA Y EL DELITO, *Manual de seguridad dinámica e inteligencia penitenciaria,* ONU, Viena, 2015, pág. 7.

3. Véase Lobato, R. M., García-Coll, J., *La encrucijada entre la radicalización y la desradicalización. Teorías, herramientas y aspectos aplicados*, Los Libros de la Catarata, Madrid, 2022.

uso de la violencia para alcanzar los objetivos ideológicos, políticos o religiosos que difunden tales creencias.

Se trata de un proceso caracterizado por no ser lineal ni uniforme, más bien al contrario, en él, se presentan diferentes trayectorias y velocidades dependiendo no solo del sujeto sino también de aquellas circunstancias personales y contextuales en las que se desarrollan las fases de esa radicalización.

Se trata, pues, de un fenómeno multicausal que combina factores estructurales, sociales, psicológicos y situacionales, y cuya complejidad exige un análisis interdisciplinar[4]. Si bien, como veremos a continuación, son múltiples los factores de riesgo que intervienen en el proceso de radicalización, habitualmente se habla de marginalidad socioeconómica, exclusión social, discriminación, ya sea real o percibida, y falta de oportunidades, elementos que al combinarse con experiencias de victimización o con entornos radicalizados que justifican la violencia, pueden facilitar que un sujeto convencional transite hacia posiciones de corte extremista[5].

En el caso del extremismo de corte yihadista, este suele apoyarse en lazos emocionales en los que la pertenencia al grupo supone un nexo de unión inquebrantable que hace que el sujeto sea capaz de cualquier acción por el grupo que integra y del que se siente parte. Si a esta situación le sumamos el entorno penitenciario, no podemos dejar de apreciar que la radicalización en estos espacios provoca desafíos particulares. El medio cerrado, la convivencia forzada con otros internos, algunos de ellos ya radicalizados incluso y las limitaciones de recursos tanto humanos como en materia de programas de reinserción que sufren nuestros centros penitenciarios, pueden favorecer la aparición de procesos tanto de captación como de adoctrinamiento, motivo por el cual, se hace necesaria la combinación de medidas preventivas, intervenciones específicas y un seguimiento exhaustivo de la persona que sale del medios penitenciario con el objetivo de evitar la reincidencia o bien que realice una primera acción terrorista[6].

Así lo expuesto, resulta claro que la radicalización de cualquier tipo, y especialmente aquella de corte yihadista, en los centros penitenciarios puede ser un factor desestabilizador de la paz social siendo uno de los principales desafíos, como ya se ha indicado, no solo la reeducación y reinserción del sujeto, sino la detección del propio proceso de radicalización que este puede sufrir y que suele darse de forma gradual e incluso entremezclado con la propia religión que profesa este. No podemos olvidar tampoco que, la prisión, como meca-

4. *Ibid*., pág. 21.

5. Schmid, A. P., *Radicalisation, De-Radicalisation, Counter-Radicalisation: A Conceptual Discussion and Literature Review*, International Centre for Counter-Terrorism, La Haya, 2013, pág. 18.

6. UNODC, *Manual de seguridad dinámica e inteligencia penitenciaria*, Oficina de las Naciones Unidas contra la Droga y el Delito, Viena, 2015, pág. 7.

nismo de control social formal, tiene una función sancionadora, pero también tiene un importante papel en la prevención y tratamiento del delito, así como en la futura reinserción de los internos. Pero como se ha indicado, el entorno penitenciario también puede ser una tierra abonada en la que germinen nuevos delitos y esto aplica también al fenómeno de la ideología extremista y de la radicalización violenta. Esta situación es tan compleja y preocupante que ha despertado el interés de instituciones europeas como Europol, quien en su informe TE-SAT 2023 advierte sobre la creciente amenaza que representan las redes de proselitismo yihadista dentro de los centros penitenciarios[7].

Este tipo de radicalización se impulsa por una gran tipología de factores pudiendo destacarse los estructurales como el hacinamiento existente en algunos de nuestros centros penitenciarios, la falta de programas de intervención así como todo lo que rodea a su aplicación, y la vulnerabilidad psicológica que afecta a muchos internos[8]. Como no puede ser de otra forma, este tipo de entornos facilitan la influencia de individuos ya radicalizados sobre otros internos que sean susceptibles de escuchar sus cantos de sirena, generando así células que pueden provocar actos de carácter delictivo dentro y fuera del sistema penitenciario. Para poder evitarlo, una estrategia fundamental es el conocimiento de los factores de riesgo y de protección que se dan en los internos a fin de poder establecer estrategias que eviten la radicalización, pero ¿cuál es el perfil de una persona que puede ser objetivo de radicalización y, por tanto, delinquir dentro del propio entorno penitenciario? Esta dificultad tiene un añadido más y es la escasa formación específica que, en muchos casos, tiene el personal de instituciones penitenciarias. Como vemos, todo suma para favorecer el proceso de radicalización en el entorno penitenciario siendo considerados como espacios especialmente vulnerables a la propagación del extremismo de carácter violento debido a sus características estructurales, sociales y psicológicas[9].

## 2.1. Factores de riesgo en los centros penitenciarios: una visión general

Atendiendo a Farrington[10], podemos decir que un factor de riesgo es cualquier característica individual o ambiental que de alguna forma se asocia a

7. EUROPOL, *Informe sobre la situación y las tendencias del terrorismo en la Unión Europea 2023* (TE-SAT), Europol, La Haya, 2023.

8. FUNDEA, *Radicalización violenta y prisión,* Cuaderno AUROÁRABE, Fundación Euroárabe, 2023.

9. Véase Basra, R., Neumann, P. R., *Prisiones y terrorismo: Gestión de delincuentes extremistas en 10 países europeos*, Centro Internacional para el Estudio de la Radicalización, Departamento de Estudios de Guerra, King's College London, 2020.

10. Farrington, D. P., *Explaining and preventing crime: The globalization of knowledge*. Criminology, 38(1), 2000, págs. 1-24.

un resultado no deseado con una mayor probabilidad. Atendiendo a diversas teorías criminológicas, hablaríamos de factor de riesgo para referirnos a una característica, condición o variable que provoca el aumento de la probabilidad de que un sujeto se involucre en una conducta de tipo delictivo no siendo necesario que el nexo causal entre el delito y la característica sea directo y pudiendo ser estos factores de corte individual, familiar, social o ambiental.

Respecto de estos factores de riesgo, que son individuales y multifactoriales, pueden clasificarse de la siguiente forma en el entorno penitenciario:

a) Aislamiento y vulnerabilidad del interno: la soledad, la pérdida de vínculos familiares y/o sociales, así como la falta de un sentido vital, pueden hacer al interno más vulnerable al discurso de captación ideológica llegando a poder ver la prisión como una oportunidad para rehacer su identidad, lo cual, sin duda, facilita la atracción al discurso del yihadismo extremista.

b) Condiciones estructurales del centro penitenciario: situaciones como el hacinamiento, las carencias en la atención sanitaria, el escaso cuidado de la salud mental, la insuficiencia de recursos materiales y educativos, la escasez de personal debidamente formado en materia de detección temprana relacionada con la radicalización, entre otros, son vectores que pueden favorecer el surgimiento de subculturas radicalizadas relacionadas con el yihadismo[11]. En este sentido, se hace inevitable hacer mención a la necesidad de formación por parte del personal de Instituciones Penitenciarias para cuestiones básicas como diferenciar una práctica religiosa de una señal real de radicalización y para ello se hace necesaria la existencia de protocolos claros y formación continuada y actualizada para detectar tales conductas.

c) La influencia de referentes radicalizados: la existencia de otros internos que actúen como referentes y que se encuentren radicalizados aprovechando su influencia para captar a otros internos hacia la yihad supone un problema de gran calado sobre todo teniendo en cuenta la vulnerabilidad de muchos internos, así como el propio proceso de socialización carcelaria que suele ser aprovechado por estos referentes radicalizados para captar a futuros miembros.

d) Necesidad de protección y de pertenencia: la adhesión a grupos extremistas de carácter yihadista puede ser estratégica, cuando el sujeto busca protección, o ideológica, en la mayoría de los casos después de un proceso más o menos largo de adoctrinamiento. Esta adhesión crea en los internos vulnerables una sensación de pertenencia a un grupo de pares con el que se siente fuerte y reconocido por los demás.

11. Véase Fernández, C., *La doble problemática del terrorismo yihadista en prisión: Una aproximación crítica a la respuesta del sistema penitenciario español*, Revista Indret, 2020.

e) Las comunicaciones de contenido yihadista: no siempre es sencillo evitar la circulación de textos, audios e incluso vídeos de contenido yihadista dentro de la prisión que ayudan a reforzar posicionamientos radicales.

## 2.2. Situación en las prisiones españolas

Según el informe *Prisiones y terrorismo. Gestión de delincuentes extremistas en diez países europeos*[12], España cuenta con una de las poblaciones penitenciarias más numerosas del continente. Entre sus internos se incluyen personas condenadas por delitos de terrorismo de corte yihadista, antiguos miembros de la extinta E.T.A. y también reclusos que, aun no habiendo sido procesados por terrorismo, se encuentran en fase de monitorización debido a indicios preocupantes de una posible radicalización violenta. El documento señala que más del 50 % de los presos actualmente considerados extremistas no ingresaron en prisión por delitos de terrorismo, sino que iniciaron su proceso de radicalización dentro del propio centro penitenciario. Este dato sitúa a los centros penitenciarios españoles como entornos de alto potencial para la captación y el adoctrinamiento, obligando a la administración penitenciaria a enfrentarse al dilema entre dispersar a estos internos para impedir la formación de focos de radicalización, o bien agruparlos en módulos específicos, con el riesgo de reforzar entre ellos el sentimiento de comunidad, victimización y martirio.

A ello se suman otros desafíos como la limitada cobertura de los programas de intervención en materia de radicalización[13], así como la descentralización del sistema penitenciario en relación con Cataluña y, más recientemente, con el País Vasco. Esta fragmentación competencial dificulta la fluidez en el intercambio de datos, genera desigualdades en la implementación del programa y complica la creación de protocolos homogéneos. Las carencias también afectan a las herramientas de evaluación del riesgo, que no siempre están actualizadas ni adaptadas a las nuevas formas de radicalización, y a la insuficiencia de personal especializado en inteligencia penitenciaria, psicología y mediación cultural. Todo ello limita la capacidad de detección temprana, la intervención eficaz y el seguimiento posterior, incrementando la dificultad de contener y revertir los procesos de radicalización en el entorno penitenciario español.

Las principales críticas, que, con objeto de mejorar, podemos hacer a la gestión de la radicalización yihadista en nuestras prisiones, en la actualidad, podrían ser, de forma muy general y sucinta, las siguientes:

12. Basra, R., Neumann, P. R., *Prisiones y terrorismo..., op. cit.*

13. Recordemos que en España rige el Programa Marco para la Intervención en la Radicalización Violenta de Internos Islamistas.

a) La falta de especialización del personal de Instituciones Penitenciarias para detectar procesos de radicalización yihadista que les permita distinguir una práctica religiosa de un discurso de carácter yihadista, haciendo que la identificación de un individuo radicalizado y/o radicalizador dependa en muchas ocasiones de la intuición del funcionario.

b) Problemas de coordinación entre las diferentes Instituciones relacionadas con la radicalización yihadista (centros penitenciarios, juzgados, fuerzas y cuerpos de seguridad y servicios sociales). La falta de coordinación y fluidez en el intercambio de la información dificulta claramente el seguimiento correcto de los internos y que la intervención con los mismos sea efectiva.

c) Fragmentación de la gestión penitenciaria: el actual reparto de competencias en materia penitenciaria ha venido a dificultar la gestión de la misma. La asunción de estas competencias por parte de Cataluña y País Vasco provoca desigualdades de actuación con los internos, así como de aplicación de los programas de intervención debido a la falta de uniformidad en los criterios.

d) Plantillas insuficientes y poco preparadas para la realidad a las que se les suma una falta de recursos materiales que redunda en una sobrecarga de trabajo que dificulta atender las situaciones de riesgo.

e) La realidad de la reinserción es compleja pues los programas de reeducación no siempre pueden adaptarse a las trayectorias individuales lo suficiente y no tienen un seguimiento efectivo fuera de los centros penitenciarios. A ello debemos sumar la posibilidad de fingir una reeducación que no es tal con el objetivo de conseguir beneficios penitenciarios por parte de los internos.

f) El enfoque de la respuesta institucional al fenómeno de la radicalización en prisiones desde la perspectiva de la seguridad es absolutamente insuficiente. Es necesario un cambio de paradigma que permita una visión circular y transversal de la situación; un enfoque que incluya cuestiones criminológicas, sociales, psicológicas y culturales pues hacer frente al fenómeno de la radicalización yihadista en nuestras instituciones penitenciarias, redundaría en un beneficio social provocando sociedades más seguras y al mismo tiempo, evitaría la marginalización que puede provocar mayor radicalización.

Como vemos, la radicalización en estos entornos constituye un fenómeno de gran complejidad que necesita de respuestas especializadas y coordinadas. Las propias características de los entornos penitenciarios y otros factores a los que ya se ha hecho referencia en este mismo texto, favorecen los procesos de captación y adoctrinamiento que, de no ser detectados a tiempo, pueden llevar a la creación y consolidación de redes extremistas intramuros y aumentan la posibilidad de reincidencia o de comisión de un atentado una

vez el sujeto ha cumplido la pena impuesta. En este contexto, la inteligencia penitenciaria se presenta como una herramienta esencial para anticipar y neutralizar estas amenazas a la seguridad nacional. Su labor, no solo se limita a la recogida de datos, sino que implica la observación sistemática de comportamientos, de factores de riesgo y de protección, la detección de cambios en las dinámicas de los internos a la hora de relacionarse o de participar en actividades con otros reclusos, el análisis de las comunicaciones y la colaboración estrecha con otros niveles de inteligencia tanto policial como estratégica por sus lazos con la seguridad nacional. Esta capacidad de obtener, procesar y compartir información relevante permitiría diseñar intervenciones específicas, ajustar programas de desradicalización y establecer medidas de control que puedan minimizar, recordemos que la seguridad cero no existe, el riesgo no solo dentro de nuestros centros penitenciarios sino también fuera de sus muros. Sin una inteligencia penitenciaria eficaz, la respuesta a la radicalización sería solamente reactiva y también fragmentada perdiendo la oportunidad de actuar en las fases tempranas del proceso de radicalización.

## 3. La ENCOT 23-24 y el entorno penitenciario

Resulta evidente, tras la contextualización de la situación, la importancia que para la seguridad colectiva tiene el fenómeno de la radicalización violenta. En este contexto, desde la perspectiva del control social formal, la Estrategia Nacional contra el Terrorismo 2023-2024 (en adelante, ENCOT) se erige como el principal marco estratégico del Estado para enfrentar el terrorismo y sus procesos de radicalización. El documento, aprobado en marzo de 2024 por el Ministerio de Interior y publicado en mayo del mismo año, evoluciona desde estrategias anteriores que tenían como objetivo la neutralización de amenazas terroristas y la reducción de vulnerabilidades, a saber la EICTIR 2012, que es la primera estrategia integral contra el terrorismo en nuestro país y la ENCOT 2019, que actualiza las nuevas amenazas relacionadas con el terrorismo.

La ENCOT actual, aborda el fenómeno de la radicalización violenta desde una perspectiva estructurada y multidimensional y la sitúa dentro de la agenda de seguridad nacional. El documento reconoce que combatir este fenómeno requiere no solo capacidad operativa, sino también inteligencia, cooperación y una visión preventiva que actúe antes de que la amenaza se materialice asumiendo que la radicalización violenta no es únicamente un desafío de seguridad, sino un problema social que exige una respuesta integral, sostenida y coordinada entre todos los actores implicados subrayando que esta amenaza es transversal y, por tanto, afecta a todos los sectores de la sociedad pudiendo desarrollarse en entornos tanto físicos como digitales, lo cual multiplica su alcance y su complejidad[14].

14. MINISTERIO DEL INTERIOR, *Estrategia Nacional contra el Terrorismo 2023-2024*, Madrid, 2023, pág. 14.

La Estrategia señala como uno de sus ejes centrales, la prevención destacando la necesidad de detectar de forma temprana los signos vinculados con la radicalización violenta para lo cual, indica, es fundamental la coordinación y la cooperación entre las fuerzas y cuerpos de seguridad, los servicios de inteligencia, las instituciones penitenciarias, las entidades educativas y las organizaciones sociales. La radicalización violenta no es tratada como un fenómeno exclusivo del terrorismo de corte yihadista, sino que también incluye la violencia de extrema derecha, de extrema izquierda y otras formas emergentes de extremismo violento. Además de ello, vuelve su mirada al uso de internet y de las redes sociales como vectores a tener en cuenta en los procesos de radicalización entendiendo que estos últimos entornos, de los que participa, un amplísimo porcentaje de la sociedad española actual, permiten la difusión masiva y a bajo coste de la propaganda extremista facilitando la captación a distancia e incluso, la auto radicalización o auto adoctrinamiento siendo necesario, en este marco, fortalecer las capacidades de vigilancia digital, desarrollar contra narrativas eficaces y colaborar con plataformas tecnológicas para limitar la difusión de contenidos extremistas, siempre garantizando el respeto a los derechos fundamentales.

En materia operativa, la Estrategia establece cuatro ámbitos de acción: prevención, ámbito en el que plantea medidas como la formación de profesionales en contacto con colectivos vulnerables, el impulso de proyectos comunitarios de cohesión social y la atención a víctimas como elemento disuasorio del extremismo en una mezcolanza de instrumentos de control social formal en combinación con estructuras de control social informal; protección; persecución y respuesta orientada a eliminar las causas y factores que favorecen la radicalización. La protección, se centra en salvaguardar a la población y las infraestructuras críticas subrayándose la importancia de los instrumentos jurídicos y policiales para desarticular redes y cortar sus fuentes de financiación; la persecución, busca neutralizar las capacidades operativas de los grupos terroristas; por último, la respuesta persigue minimizar los efectos de un ataque y restaurar la normalidad y la convivencia pacífica. Todo ello sin olvidar la importancia de la cooperación internacional, pues la radicalización violenta y su expresión a través del terrorismo no conoce fronteras y por tanto debe reforzarse la cooperación y coordinación con organismos de la Unión Europea, así como otros internacionales, señalando la necesidad de integrar el concepto de resiliencia social como instrumento para contrarrestar el extremismo violento. Sin duda, una sociedad cohesionada con una fuerte estructura de valores democráticos es menos permeable a la propaganda extremista por lo que la educación en valores, el pensamiento crítico y la sensibilización comunitaria se señalan como barreras de contención frente al extremismo[15].

En el ámbito penitenciario, la ENCOT reconoce que los centros penitenciarios son especialmente vulnerables pues el contacto directo con individuos

15. MINISTERIO DEL INTERIOR, *Estrategia Nacional..., op. cit.,* pág. 35.

radicalizados, la existencia de conflictos identitarios o la influencia de líderes carismáticos pueden favorecer la captación intramuros, lo que supone un riesgo para la seguridad colectiva. Ello hace necesaria la implementación de una suerte de inteligencia que impidan que nuestras prisiones puedan convertirse en incubadoras de extremismo. Tal y como determina la UNODC, «la inteligencia penitenciaria constituye una herramienta imprescindible para identificar y neutralizar actividades extremistas antes de que alcancen un punto crítico[16]».

La Estrategia identifica, que son los condenados por delitos de terrorismo que mantienen su ideología extremista, los internos en proceso de radicalización y los individuos no radicalizados pero vulnerables a los discursos extremistas en base a los factores de riesgo que se nombraron en páginas anteriores, los que representan un potencial riesgo para la seguridad colectiva. Para hacer frente a esta problemática, la ENCOT, plantea una suerte de inteligencia penitenciaria a la que se alude como un conjunto de actividades de obtención, análisis y explotación de información relacionada con dinámicas y conductas cercanas a la radicalización e interconectada con el intercambio de información con otras instituciones[17]. De esta forma se busca detectar de forma temprana los signos de radicalización, observando el comportamiento y las relaciones de los internos; evaluar el riesgo individual de cada usuario del centro penitenciario con riesgo de radicalización con base en herramientas específicas y adaptadas a la realidad penitenciaria española e implementar medidas, en unos casos de dispersión y en otros de agrupación controlada, con el objetivo de minimizar la expansión de la ideología radical. Además de lo expuesto, y con base en el artículo 25.2[18] de la Constitución Española en cuanto a la reeducación y reinserción como fines de las penas privativas de libertad, se pone de manifiesto la importancia de los programas de interven-

16. UNODC, *Manual de seguridad dinámica e inteligencia penitenciaria*, Oficina de las Naciones Unidas contra la Droga y el Delito, Viena, 2015, pág. 5.

17. En consonancia con las recomendaciones de la Oficina de Naciones Unidas contra la Droga y el Delito (UNODC), la estrategia destaca que la inteligencia penitenciaria debe integrarse en un sistema más amplio de seguridad e intercambio de información entre administraciones (UNODC, Manual de seguridad dinámica e inteligencia penitenciaria, Viena, 2015, pág. 5.). Lo que implica superar barreras derivadas de la descentralización penitenciaria en Cataluña y más recientemente en País Vasco y garantizar protocolos homogéneos en todo el territorio nacional.

18. Artículo 25.2 CE: *Las penas privativas de libertad y las medidas de seguridad estarán orientadas hacia la reeducación y reinserción social y no podrán consistir en trabajos forzados. El condenado a pena de prisión que estuviere cumpliendo la misma gozará de los derechos fundamentales de este Capítulo, a excepción de los que se vean expresamente limitados por el contenido del fallo condenatorio, el sentido de la pena y la ley penitenciaria. En todo caso, tendrá derecho a un trabajo remunerado y a los beneficios correspondientes de la Seguridad Social, así como al acceso a la cultura y al desarrollo integral de su personalidad*.
«BOE» núm. 311, de 29/12/1978.

ción en línea con instrumentos que combinan acciones psicológicas, educativas y culturales que permitan ayudar a desmontar las bases ideológicas que legitiman la violencia. Tras el trabajo en prisión con los internos, la ENCOT señala la necesidad también de un trabajo postpenitenciario de prevención en el que el seguimiento evite recaída o el reingreso en alguna red extremista, todo ello bajo el paraguas del respeto a los derechos fundamentales.

## 4. Inteligencia penitenciaria: detección y seguimiento

Si bien en origen, la inteligencia se constituyó como una herramienta fundamental para la seguridad, en la actualidad alcanza a los más diversos ámbitos, no solo de seguridad, sino también económicos, industriales, etcétera. El objetivo de la inteligencia no es solo describir la realidad, sino que permite anticipar las amenazas, identificar vulnerabilidades y ofrecer bases sólidas de actuación eficaz en cualquier contexto no pudiendo confundirse en caso alguno como una acumulación de datos pues se trata de un proceso analítico y estructurado que transforma informaciones en conocimiento útil para el proceso de toma de decisiones.

En el ámbito de la seguridad y la defensa, es especialmente necesaria ya que la inteligencia permite el diseño de estrategias preventivas y de acción contra fenómenos de todo tipo que perturban la convivencia humana siendo su valor esencial la anticipación y la reducción de incertidumbre. Si trasladamos lo expuesto al entorno penitenciario, la inteligencia puede adquirir un valor muy relevante en la prevención y la contención de dinámicas y conductas que puedan poner en peligro la seguridad dentro de los muros del centro penitenciario pero también fuera de estos cuando se produce el fin de la condena del sujeto y este es puesto en libertad. En este sentido, la Oficina de las Naciones Unidas contra la Droga y el Delito, afirma que la inteligencia penitenciaria es un componente catalogado como esencial en la gestión de la seguridad de los centros penitenciarios pues permite identificar y neutralizar actividades ilícitas o de carácter extremistas antes de que alcancen un punto de desarrollo crítico[19] convirtiéndose así la inteligencia en un instrumento al servicio de la seguridad nacional y de la protección de la ciudadanía.

Siguiendo con lo expuesto, podemos definir entonces la inteligencia desarrollada en el entorno penitenciario como el conjunto de actividades sistémicas de recogida de información relevante y análisis de la misma sobre personas, hechos o conductas que se producen en el interior del centro penitenciario y que tiene como objetivo la prevención, detección y neutralización de cualquier amenaza para la seguridad del propio centro o de la seguridad colectiva. En el caso concreto de la radicalización violenta de contenido yihadista, este tipo de inteligencia es estratégica pues puede evitar la radicali-

19. UNODC, *Manual de seguridad, op. cit.*, pág. 5.

zación de los sujetos. En España, lo que podríamos denominar inteligencia en el entorno penitenciario, se sustenta en tres elementos fundamentales: la observación directa por parte de los funcionarios de vigilancia y tratamiento dentro del centro penitenciario, el análisis técnico de la información que pueda ser recogida y por último, la coordinación con otras partes del engranaje de la seguridad y defensa de nuestro país que puedan verse implicados en estas dinámicas. Este trabajo implica la integración de conocimiento operativo y de análisis estratégico con el objetivo de poder generar medidas que permitan la gestión de la situación de forma segura y efectiva[20].

Respecto a la detección de indicios de radicalización puede apoyarse en indicadores como los cambios repentinos en las creencias religiosas o políticas del usuario del centro penitenciario, la adopción por parte de este de discursos violentos o excluyentes, la ruptura de vínculos familiares o del grupo de pares previos, el rechazo a participar en actividades comunes, el intento de influir ideológicamente en otros internos, la recepción, uso o difusión de material propagandístico o de comunicaciones con el exterior que puedan ser susceptibles de sospecha. Atendiendo al Programa Marco para la Intervención en la Radicalización Violenta de Internos Islamistas, elaborado por la Secretaría General de Instituciones Penitenciarias[21], la identificación temprana de este tipo de indicadores permite establecer las medidas de seguimiento y tratamiento pertinentes y adaptadas al nivel de riesgo del interno.

Por su parte, el seguimiento, implica la monitorización del usuario del centro penitenciario a través de entrevistas periódicas, control de comunicaciones escritas y telefónicas siempre atendiendo a la normativa vigente con el objetivo de no vulnerar los derechos fundamentales del interno, análisis de sus interacciones en módulos, y revisión de su evolución en los programas de tratamiento. La fase de seguimiento es importante para evaluar si las medidas aplicadas hasta el momento en la fase de detección han sido o no eficaces y todo ello con el objetivo de determinar el potencial riesgo a la seguridad del interno, es decir, si presenta algún tipo de avance que pueda llevar a pensar en la desradicalización o si, por el contrario, las medidas no han surtido efecto y el sujeto ha aumentado su grado de compromiso con la ideología radical. Si bien es cierto, en palabras de Vidino[22] que la radicalización es un proceso dinámico y reversible, lo cierto es que revertirlo conlleva una intervención prolongada que es necesario adaptar al contexto del recluso.

A estas dos fases habría que sumar el plano operativo; la inteligencia en el contexto penitenciario no puede actuar de forma aislada y por tanto necesita

20. UNODC, *Manual de seguridad, op. cit.*, pág. 9.

21. SECRETARÍA GENERAL DE INSTITUCIONES PENITENCIARIAS, *Programa Marco para la Intervención en la Radicalización Violenta de Internos Islamistas*, Ministerio del Interior, Madrid, 2016, pág. 14.

22. Vidino, L., *Prison Radicalization in Western Europe: Assessing the Policies of 12 Countries*, George Washington University, Washington D.C., 2010, pág. 27

de un flujo constante de información en el que se combinen otros tipos de actores como servicios policiales y, desde el año 2014, el Centro de inteligencia contra el terrorismo y el crimen organizado (en adelante, CITCO)[23]. Esta interrelación entre diversos organismos va a permitir vincular la información del interior de los centros penitenciarios con investigaciones abiertas en el exterior mejorando la prevención de los delitos e incluso desactivando redes relacionadas con la radicalización de corte yihadista[24]. En esta línea, la ENCOT hace de la detección temprana y del seguimiento continuado sus pilares estratégicos ya que la prisión no es solo el espacio de cumplimiento de la condena de una persona que ha cometido un ilícito sino que, durante el tiempo que esta dure, el centro penitenciario es el lugar donde va a desarrollar relaciones sociales y en el que se pueden crear alianzas y jerarquías que pueden actuar tanto de factor de riesgo como de factor de protección para la propagación de ideas extremistas[25].

En este sentido, la Estrategia propone como medida preventiva la detección temprana, es decir, que esa detección comience con observar conductas básicas como cambios graduales en el discurso, hábitos, relaciones y rutinas del interno. Ello implicaría identificar señales como por ejemplo:

a) el aislamiento voluntario del grupo habitual y la creación de círculos cerrados de influencia;

b) el uso recurrente de lenguaje ideológicamente violento o justificativo de la violencia;

c) el rechazo de actividades institucionales o programas de reinserción por motivos ideológicos;

d) los contactos frecuentes con internos ya identificados como radicalizados.

Para la identificación de tales conductas, serán de gran utilidad el uso de herramientas de evaluación de riesgo adaptadas al contexto penitenciario en nuestro país con las que se pueda registrar, puntuar y monitorizar tales conductas teniendo presente el vector tiempo y así, determinar el riesgo real del sujeto. En esta línea, la UNODC recomienda el uso de perfiles dinámicos que no se basen exclusivamente en antecedentes penales, sino que incluyan variables de personalidad, entorno social y comportamiento intramuros[26].

23. Creado el 15 de octubre de 2014 mediante Real Decreto 873/2014, de 10 de octubre, por el que se modifica el Real Decreto 400/2012, de 17 de febrero, por el que se desarrolla la estructura orgánica básica del Ministerio del Interior.

24. EUROPOL, *European Union Terrorism Situation and Trend Report 2023 (TE-SAT),* Europol, La Haya, 2023, pág. 41.

25. MINISTERIO DEL INTERIOR, *Estrategia Nacional..., op. cit.,* pág. 26.

26. UNODC, *Manual de seguridad, op. cit.,* pág. 11.

Como se ha señalado, tras la detección se pondrían en marcha mecanismos de seguimiento continuado con el objetivo de evaluar la evolución del interno y determinar la eficacia de las medidas que se hubieran implementado. La Estrategia señala que el seguimiento ha de ser multidisciplinar implicando a:

a) Funcionarios de vigilancia que aportan observaciones directas del comportamiento diario.

b) Equipos técnicos del centro penitenciario (juristas, psicólogos, educadores) que evalúan la adaptación social e ideológica del interno.

c) Unidades que podríamos catalogar como de inteligencia en el contexto penitenciario que cruzan información con otros centros y con fuerzas de seguridad.

Conjuntamente, plantea la posibilidad de diversas medidas operativas clave en materia de detección y seguimiento como serían:

a) Mapeo social: identificación de redes internas de influencia y jerarquías ideológicas.

b) Control de comunicaciones: análisis de correspondencia, llamadas y visitas para detectar mensajes radicales o contactos con el exterior relacionados con extremismo.

c) Observación de patrones grupales: vigilancia de actividades colectivas que puedan encubrir adoctrinamiento.

d) Intervenciones programáticas: inclusión en programas de desradicalización, mediación intercultural y terapia cognitivo-conductual.

Como señala Lobato, «la clave para neutralizar la radicalización en prisión reside en integrar la inteligencia penitenciaria en el sistema global de seguridad»[27].

## 5. Conclusiones

La radicalización violenta en el ámbito penitenciario constituye un desafío estructural y sostenido para la seguridad nacional. El análisis desarrollado en este trabajo evidencia que los centros penitenciarios, lejos de ser únicamente espacios de custodia y reeducación, pueden convertirse en focos de captación, adoctrinamiento y consolidación de redes extremistas, especialmente de corte yihadista. Factores como el hacinamiento, la vulnerabilidad psicológica de los internos, la insuficiente formación del personal y la falta de protocolos homogéneos favorecen un terreno fértil para la propagación de

27. Lobato, R. M., *Inteligencia penitenciaria y seguridad nacional*, Los Libros de la Catarata, Madrid, 2021, pág. 88.

ideologías violentas. Todo ello hace pensar en la necesidad de una suerte de inteligencia penitenciaria que permita anticipar situaciones delictivas relacionadas con los delitos de terrorismo dentro y fuera de los muros de nuestras prisiones.

La Estrategia Nacional contra el Terrorismo 2023-2024, refuerza la necesidad de esta especie de inteligencia en el entorno penitenciario especializada, capaz de detectar tempranamente los signos de radicalización, realizar un seguimiento continuado y coordinar información con otros niveles de inteligencia policial y estratégica. Este enfoque multidisciplinar, que combina medidas preventivas, operativas y de reinserción, se alinea con la idea de que la seguridad no puede entenderse exclusivamente desde la dimensión reactiva, sino que exige una anticipación basada en análisis y cooperación interinstitucional.

La Operación DIHAN[28] constituye un ejemplo paradigmático de cómo la información generada intramuros, correctamente procesada y compartida, puede tener un impacto decisivo en la neutralización de amenazas externas. Esta operación, desarrollada en España en 2015, permitió desarticular una red de captación y adoctrinamiento yihadista que operaba tanto en el exterior como en el interior de centros penitenciarios, y que utilizaba a internos radicalizados como vectores de influencia y reclutamiento. La actuación combinó inteligencia en el entorno penitenciario, vigilancia operativa y cooperación internacional, anticipando riesgos y evitando la posible materialización de atentados.

La interrelación entre la ENCOT y casos como la Operación DIHAN subraya la importancia de:

28. Véase OBSERVATORIO INTERNACIONAL DE ESTUDIOS SOBRE TERRORISMO, *Operación Dihan: Una sentencia inédita contra la radicalización yihadista en prisión,* 2025; A continuación se expone un esquema cronológico y operativo de la Operación DIHAN: A) Contexto previo (2014-2015): Los servicios de inteligencia penitenciaria y policial detectaron la existencia de internos radicalizados en varias prisiones españolas que, mediante comunicaciones cifradas y contactos con el exterior, coordinaban labores de captación y adoctrinamiento de nuevos miembros para el autodenominado Estado Islámico. B) Inicio de la operación (2015): El CITCO, en coordinación con Instituciones Penitenciarias, Guardia Civil y Policía Nacional, abrió una investigación conjunta para mapear redes internas y externas. Se analizaron comunicaciones telefónicas, correspondencia y contactos en locutorios, así como la dinámica social en módulos. C) Desarrollo operativo: Identificación de líderes radicalizados dentro de prisión que ejercían influencia sobre internos vulnerables. Localización de contactos externos en varias comunidades autónomas que proveían material propagandístico, apoyo logístico y financiación. Establecimiento de vínculos entre internos yihadistas y grupos operativos en Siria e Irak. D) Desarticulación (noviembre de 2015): Se llevaron a cabo detenciones simultáneas dentro y fuera de las prisiones. Entre los arrestados había internos en fase avanzada de radicalización y personas en libertad que actuaban como nodos de conexión. E) Resultado: Neutralización de una red con capacidad real de captar, adoctrinar y facilitar combatientes extranjeros. Intervención de material propagandístico y manuales para la comisión de atentados. Refuerzo de los protocolos de control de comunicaciones y clasificación de internos de alto riesgo.

Integrar la inteligencia en los entornos penitenciarios y a su vez en el ciclo global de inteligencia contra el terrorismo.

Establecer canales fluidos y bidireccionales de información entre prisiones, fuerzas y cuerpos de seguridad, y servicios de inteligencia.

Potenciar programas de desradicalización y seguimiento postpenitenciario, evitando la reincidencia o la integración en redes extremistas tras la excarcelación.

En definitiva, el fortalecimiento de la inteligencia aplicada al entorno penitenciario, en consonancia con los objetivos de la ENCOT y apoyado en experiencias operativas como la de DIHAN, se presenta como un pilar esencial para prevenir, contener y revertir la radicalización violenta, garantizando una respuesta integral que combine la protección de la sociedad con el respeto a los derechos fundamentales.

## BIBLIOGRAFÍA

**Basra, R.**, **Neumann, P. R.**, *Prisiones y terrorismo: Gestión de delincuentes extremistas en 10 países europeos*, Centro Internacional para el Estudio de la Radicalización, Departamento de Estudios de Guerra, King's College London, 2020.

**Borum, R.**, *Radicalization into violent extremism I: A review of social science theories*, Journal of Strategic Security, vol. 4, núm. 4, 2011.

**EUROPOL**, *European Union Terrorism Situation and Trend Report 2023 (TESAT)*, Europol, La Haya, 2023.

**Farrington, D. P.**, *Explaining and preventing crime: The globalization of knowledge*, Criminology, vol. 38, núm. 1, 2000.

**Fernández, C.**, *La doble problemática del terrorismo yihadista en prisión: Una aproximación crítica a la respuesta del sistema penitenciario español*, Revista Indret, 2020.

**FUNDEA**, *Radicalización violenta y prisión*, Cuaderno AUROÁRABE, Fundación Euroárabe, 2023.

**Lobato, R. M.**, *Inteligencia penitenciaria y seguridad nacional*, Los Libros de la Catarata, Madrid, 2021.

**MINISTERIO DEL INTERIOR**, *Estrategia Nacional contra el Terrorismo 2023-2024*, Madrid, 2023.

**OBSERVATORIO INTERNACIONAL DE ESTUDIOS SOBRE TERRORISMO**, *Operación Dihan: Una sentencia inédita contra la radicalización yihadista en prisión*, 2025.

**OFICINA DE LAS NACIONES UNIDAS CONTRA LA DROGA Y EL DELITO**, *Manual de seguridad dinámica e inteligencia penitenciaria*, ONU, Viena, 2015.

**Schmid, A. P.**, *Radicalisation, De-Radicalisation, Counter-Radicalisation: A Conceptual Discussion and Literature Review*, International Centre for Counter-Terrorism, La Haya, 2013.

**SECRETARÍA GENERAL DE INSTITUCIONES PENITENCIARIAS**, *Programa Marco para la Intervención en la Radicalización Violenta de Internos Islamistas*, Ministerio del Interior, Madrid, 2016.

**Vidino, L.**, *Prison Radicalization in Western Europe: Assessing the Policies of 12 Countries*, George Washington University, Washington D.C., 2010.

# DEL INFORME DRAGHI (O LA BRÚJULA PARA LA COMPETITIVIDAD) A LA ACCIÓN: ¿UNA DIVISIÓN DE INTELIGENCIA ECONÓMICA EN LA COMISIÓN EUROPEA?

**Diego González López**

*Profesor e investigador predoctoral (ACIF)*
*Universidad de Valencia*
*Vocal académico de la Asociación de Jóvenes en Inteligencia, Defensa y Seguridad (INDESEC)*

## 1. Introducción

La Unión Europea (en adelante, UE) se encuentra en un momento crucial de su desarrollo histórico. La transformación del orden internacional, marcada por la rivalidad entre grandes potencias, la aceleración tecnológica y las tensiones geopolíticas[1], ha puesto en evidencia las debilidades estructurales del modelo europeo. Las sucesivas crisis —desde la financiera de 2008 hasta la pandemia de COVID-19, pasando por la guerra en Ucrania y la tormenta arancelaria desatada por Donald Trump— han demostrado que la UE carece de instrumentos suficientes para anticipar riesgos y responder de manera coordinada y eficaz. En este escenario, en el que «lo único previsible es la imprevisión»[2], la competitividad ya no puede entenderse únicamente en términos económicos, sino como un factor esencial para la autonomía estratégica y la resiliencia de la UE.

1. Véase López Canorea, A., Marrades, A., González Márquez, J., *La pugna por el nuevo orden internacional. Claves para entender la geopolítica de las grandes potencias*, Barcelona, Espasa, 2023.

2. Sahagún, F., «¿Declive o recomposición de Occidente? en Beneyto, J. M. (dir.): *¿Hacia un nuevo orden mundial? La guerra de Ucrania y sus consecuencias*, Barcelona, Deusto, 2022, pág. 333.

En 2023, la presidenta de la Comisión Europea, Ursula von der Leyen, encomendó a Mario Draghi la elaboración de un informe sobre el futuro de la competitividad europea. El documento, presentado en septiembre de 2024 bajo la rúbrica «El futuro de la competitividad en Europa», constituye un punto de inflexión sobre la futura orientación estratégica de la UE. El llamado Informe Draghi no solo diagnostica la pérdida relativa de competitividad frente a Estados Unidos y China, sino que reclama un salto cualitativo en inversión, innovación y coordinación institucional. Con más de 170 medidas, el informe dibuja una hoja de ruta ambiciosa que exige a la UE reflexionar sobre su futuro y actuar en consecuencia.

Ahora bien, la eficacia de estas recomendaciones dependerá de la capacidad de la UE —y, en particular, de la Comisión Europea— para transformarlas en políticas concretas y sostenibles. En este punto emerge una cuestión fundamental: ¿Dispone la Comisión Europea de los mecanismos de acción necesarios para alcanzar sus objetivos estratégicos? En otras palabras, ¿cuenta con un órgano especializado en materia de inteligencia que, efectuando el ciclo de inteligencia, facilite la toma de decisiones orientadas a la defensa de sus intereses? La respuesta es negativa. Aunque existen órganos especializados en ámbitos técnicos y sectoriales, su perspectiva es fragmentaria y parcial, y ninguno de ellos produce inteligencia en sentido estricto —es decir, no realizan el ciclo de inteligencia—.

Por ejemplo, aunque cada Comisario dispone de un gabinete propio, que a su vez trabaja en estrecha colaboración con las distintas Direcciones Generales de la Comisión Europea (conocidas como DG)[3], este esquema presenta limitaciones evidentes. Aun siendo una estructura adecuada y valiosa, no proporciona a los comisarios una visión de conjunto sobre los desafíos estratégicos de la UE.

Este vacío institucional abre la posibilidad de plantear nuevas soluciones. Entre ellas, la creación de una División de Inteligencia Económica (*Economic Intelligence Division*) dentro de la Comisión Europea se presenta como una opción a considerar. Tal iniciativa permitiría reforzar la capacidad de la UE para analizar su posición en un mundo competitivo, ofrecer apoyo estratégico directo a los comisarios y contribuir a la implementación efectiva de las propuestas formuladas en el Informe Draghi o en la Brújula para la Competitividad[4].

El objetivo de este trabajo es, por tanto, explorar la viabilidad y conveniencia de establecer un órgano de inteligencia económica en el seno de la Comisión Europea. Asimismo, se plantea una alternativa: la transformación del *Joint Research Centre* (JRC).

3. <https://www.hablamosdeeuropa.es/es/Paginas/La-Comision.aspx> [última consulta: 17 de agosto de 2025].

4. <https://www.consilium.europa.eu/es/policies/competitiveness-compass/> [última consulta: 17 de agosto de 2025].

# 2. Consideraciones previas

Antes de abordar la propuesta de creación de una División de Inteligencia Económica en la Comisión Europea —y su posible alternativa—, resulta imprescindible contextualizarla. Para ello, conviene examinar previamente el sistema competencial de la UE y el papel específico de la Comisión Europea en el entramado comunitario, así como realizar una aproximación a las estructuras de inteligencia actualmente existentes. De igual modo, se define el concepto de inteligencia económica y, por último, se destaca el Informe Draghi como un llamamiento a la acción en el plano geoeconómico de la UE.

## 2.1. El sistema competencial de la Unión Europea

La UE está integrada actualmente por 27 Estados miembros, tras la salida del Reino Unido e Irlanda del Norte el 31 de enero de 2020. Su origen institucional puede ubicarse en el Tratado de París de 1951, que dio lugar a la Comunidad Europea del Carbón y del Acero (CECA), y en el Tratado de Roma de 1957, mediante el cual nacieron la Comunidad Económica Europea (CEE) y la Comunidad Europea de la Energía Atómica (EURATOM).

Posteriormente, el 8 de abril de 1965, las tres comunidades se integraron en una sola estructura: la Comunidad Europea (en adelante CE). En este proceso, España pasó a formar parte de la CE con la entrada en vigor, el 1 de enero de 1986, del Tratado de Adhesión. El gran salto se produjo con el Tratado de Maastricht de 1992, que dio lugar a la actual UE articulada en tres pilares: la Comunidad Europea, la Política Exterior y de Seguridad Común (en adelante PESC) y la cooperación en justicia y asuntos de interior (JAI). Sin embargo, el Tratado de Lisboa de 2007 transformó este esquema, sustituyendo los tres pilares por un sistema basado en categorías competenciales que reflejan el grado de cesión de soberanía de los Estados miembros a la UE.

De acuerdo con el TFUE, se distinguen tres grandes tipos de competencias: exclusivas, compartidas y de apoyo o coordinación. El apartado primero del art. 2 del Tratado de Funcionamiento de la Unión Europea (en adelante TFUE) establece: *«Cuando los Tratados atribuyan a la Unión una competencia exclusiva en un ámbito determinado, sólo la Unión podrá legislar y adoptar actos jurídicamente vinculantes, mientras que los Estados miembros, en cuanto tales, únicamente podrán hacerlo si son facultados por la Unión o para aplicar actos de la Unión»*. Estas competencias abarcan materias como la unión aduanera, la política comercial común, la política monetaria de los Estados miembros de la eurozona, la conservación de recursos biológicos marinos y determinados acuerdos internacionales (art. 3.1 TFUE).

Las competencias compartidas se regulan en el art. 4 TFUE, donde se señala que la Unión *«dispondrá de competencia compartida con los Estados miembros cuando los Tratados le atribuyan una competencia que no*

*corresponda a los ámbitos mencionados en los artículos 3 y 6»*. Esta categoría cubre áreas de gran relevancia como el mercado interior, la política social, la cohesión económica, social y territorial, la agricultura y la pesca (salvo la conservación de los recursos biológicos marinos), el medio ambiente, la protección de los consumidores, los transportes, las redes transeuropeas, la energía, el espacio de libertad, seguridad y justicia, así como la seguridad en materia de salud pública (art. 4.2 TFUE). Conviene subrayar que, en virtud del apartado segundo del art. 2 TFUE, cuando la UE ejerce una competencia compartida, los Estados miembros solo pueden intervenir en la medida en que la Unión no lo haya hecho.

El art. 6 TFUE establece los ámbitos en los que la UE únicamente puede apoyar, coordinar o complementar la acción de los Estados miembros, como son la salud pública, la industria, la cultura, el turismo, la educación y la formación profesional, la juventud y el deporte, la protección civil y la cooperación administrativa. Asimismo, los apartados tercero y cuarto del art. 4 TFUE precisan que, en materia de investigación, desarrollo tecnológico, espacio, cooperación al desarrollo y ayuda humanitaria, la acción de la UE no impide el ejercicio de competencias nacionales.

Existe, no obstante, un régimen particular en el terreno de la PESC, en el que rige la unanimidad del Consejo Europeo. Sin embargo, el papel del Parlamento Europeo y de la Comisión Europea resulta muy limitado. Esto obedece a que los Estados miembros no han puesto en común su soberanía en estos ámbitos. Al encontrarse la inteligencia estrechamente ligada a la defensa y la seguridad, es decir, a la PESC, esto explica que no existe ningún servicio común de inteligencia en el ámbito de la UE. En su lugar, se han desarrollado simples agencias de carácter analítico, como el Centro de Situación e Inteligencia de la Unión Europea (EU INTCEN).

## 2.2. La Comisión Europea

La Comisión Europea, con sede en Bruselas (Bélgica), constituye el órgano ejecutivo de la Unión Europea y representa el interés general del conjunto de los Estados miembros. Su función principal consiste en ejercer la iniciativa legislativa —es decir, proponer normas que luego deberán ser debatidas y aprobadas por el Consejo de la Unión Europea y el Parlamento Europeo— y en garantizar la correcta aplicación de los Tratados, de la legislación derivada y del presupuesto comunitario[5].

A estos efectos, la Comisión actúa como motor político, ya que es la institución encargada de transformar los grandes objetivos estratégicos de la UE

5. <https://www.hablamosdeeuropa.es/es/Paginas/La-Comision.aspx> [última consulta: 17 de agosto de 2025].

en propuestas legislativas y programas de acción concretos. Se compone de 27 comisarios (uno por cada Estado miembro):

a) un presidente;

b) tres vicepresidentes ejecutivos;

c) un Alto Representante para Asuntos Exteriores y Política de Seguridad con rango de vicepresidente;

d) 4 vicepresidentes;

e) 18 comisarios.

Ahora bien, conviene matizar que, si bien la Comisión posee una enorme capacidad de influencia a la hora de fijar la agenda política y elaborar propuestas normativas, el poder de decisión último no recae en ella. La aprobación de las leyes europeas requiere la participación del Consejo de la Unión Europea (donde están representados los gobiernos nacionales) y del Parlamento Europeo (como institución representativa de la ciudadanía).

## 2.3. La estructura de inteligencia europea

La inteligencia (como producto) es la información útil, pertinente y elaborada para la toma de decisiones. El ciclo de inteligencia, dividido en cinco fases, hace referencia al proceso mediante el que se articula su producción. Las fases del ciclo de inteligencia son las siguientes[6]:

a) planificación y dirección: determinación de las necesidades de inteligencia;

b) obtención de información: explotación de información: explotación de las fuentes de información;

c) procesamiento de la información: análisis técnico, almacenamiento, control, etc.;

d) producción de inteligencia: integración, interpretación y difusión;

e) retroalimentación: compartir la utilidad de la inteligencia.

A diferencia de lo que ocurre en los Estados miembros, la Unión Europea carece de un servicio de inteligencia común —es decir, no cuenta con un servicio capaz de desarrollar el ciclo de inteligencia por sí mismo[7]—. Y es que, la seguridad nacional sigue siendo una competencia exclusiva de cada Estado miembro conforme al artículo 4.2 del TUE.

---

6. De Castro García, A., «Ciclo de inteligencia» en Díaz Fernández, A. M. (dir.): *Conceptos fundamentales de inteligencia*, Valencia, Tirant lo Blanch, 2016, págs. 53-55; González López, D., La integración europea en materia de inteligencia: ¿un servicio de inteligencia europeo?, *Studia Humanitatis Journal*, vol. 4, núm. 2, 2024, pág. 8.

7. *Ibid*., pág. 17.

Ello no significa, sin embargo, que no existan mecanismos de cooperación y análisis de inteligencia. La arquitectura europea se compone de diversos órganos y agencias con funciones parciales, entre los que destacan:

a) el Centro de Situación e Inteligencia de la Unión Europea (en adelante EU INTCEN);

b) el Centro de Satélites de la Unión Europea (SatCen);

c) el Estado Mayor de la Defensa de la Unión Europea;

d) la Agencia de Ciberseguirdad de la Unión Europea (ENISA);

e) el Colegio de Inteligencia en Europa (*Intelligence College in Europe*).

En el ámbito policial y judicial, destacan Europol y su Centro Europeo Contra el Terrorismo (ECTC), así como Eurojust, ambos orientados a reforzar la cooperación entre autoridades nacionales frente a la delincuencia transfronteriza y el terrorismo. Sin embargo, estas agencias no desarrollan inteligencia en sentido estricto, sino que se centran en la coordinación operativa y en el intercambio de información entre Estados miembros.

Actualmente, el verdadero núcleo analítico de la UE en materia de inteligencia es el EU INTCEN, conocido hasta 2012 como Centro de Situación (SITCEN). Su foco es la seguridad y la defensa, no la competitividad económica de la UE, y su trabajo se basa fundamentalmente en el procesamiento de información procedente de los Estados miembros y de fuentes abiertas, sin capacidad autónoma de obtención de inteligencia sobre el terreno.

Como señala Díaz-Caneja Greciano, el EU INTCEN se encuentra compuesto por aproximadamente una centena de personas, y su misión consiste en proporcionar análisis de inteligencia, productos de alerta temprana y conocimiento de la situación al Alto Representante para Asuntos Exteriores y Política de Seguridad, al Servicio Europeo de Acción Exterior (SEAE) y, en determinados casos, a altos cargos de la UE[8].

En definitiva, la UE dispone de una serie de mecanismos fragmentados que cubren áreas específicas —imágenes satelitales, ciberseguridad, cooperación policial, etc.—, pero que no constituyen un verdadero servicio de inteligencia europeo. Existe una clara voluntad de coordinación y de puesta en común de información, aunque persiste una limitada capacidad autónoma de obtención y producción de inteligencia en sentido estricto, lo que genera una dependencia estructural de la información suministrada por los Estados miembros y, en ocasiones, por actores externos como Estados Unidos o Reino Unido[9].

Este déficit supone una carencia estructural que condiciona la autonomía estratégica de la UE y, en particular, deja sin cubrir adecuadamente un

8. Díaz-Caneja Greciano, J. M., La cooperación de inteligencia en la Unión Europea. *Boletín Instituto Español de Estudios Estratégicos*, núm. 6, 2014, pág. 8.

9. *Ibid*., pág. 10.

ámbito crucial: la inteligencia económica. Un mecanismo indispensable para orientar las decisiones de la Comisión Europea (y de las demás instituciones) en defensa de los intereses comunes europeos.

## 2.4. Inteligencia competitiva vs. inteligencia económica

Si bien el objetivo de este trabajo es proponer la creación de un órgano de inteligencia destinado a apoyar la toma de decisiones de la Comisión Europea en un contexto marcado por la necesidad de avanzar en los intereses estratégicos vinculados al refuerzo de la competitividad, resulta imprescindible establecer previamente una distinción conceptual entre inteligencia competitiva e inteligencia económica.

Según el Equipo Económico del Centro Nacional de Inteligencia (CNI), la inteligencia competitiva se concibe como una herramienta de gestión o práctica empresarial que consiste en un proceso sistemático, estructurado, legal y ético por el que se recoge y analiza información que, una vez convertida en inteligencia, se difunde a los responsables de la decisión para facilitar la misma, de forma que se mejora la competitividad de la empresa, su poder de influencia y su capacidad de defender sus activos materiales e inmateriales[10]. Sin embargo, no hay que confundir la inteligencia competitiva con la inteligencia de negocio o la inteligencia económica.

Como explica Izquierdo Triana, la inteligencia de negocio (*business intelligence*), a diferencia de la inteligencia competitiva —actividad externa y enfoque cualitativo—, se centra en la actividad interna con un enfoque cuantitativo de recopilación y gestión masiva de datos[11]. Por su parte, la inteligencia económica —cuyo origen, como concepto, se remonta a Wilensky en 1967[12]— se realiza por el Estado y por las empresas[13], mientras que la inteligencia competitiva únicamente por las empresas[14]. El Informe Martre de 1994 define la inteligencia económica como el conjunto de acciones —que deben seguir el ciclo de inteligencia— coordinadas a la investigación, tratamiento y distribución, en vista a su explotación, de la información útil a los actores económicos[15].

---

10. Como se citó en Izquierdo Triana, H., «Inteligencia competitiva» en Díaz Fernández, A. M. (dir.): *Conceptos fundamentales de inteligencia*, Valencia, Tirant lo Blanch, 2016, pág. 216.

11. Izquierdo Triana, H., «Inteligencia competitiva» en Díaz Fernández, A. M. (dir.): *Conceptos fundamentales de inteligencia*, Valencia, Tirant lo Blanch, 2016, pág. 218.

12. Véase Wilensky, H., *Organizational Intelligence: Knowledge and Policy in Government and Industry,* 1967.

13. Oliver Atenas, E., «Inteligencia económica» en Díaz Fernández, A. M. (dir.): *Conceptos fundamentales de inteligencia*, Valencia, Tirant lo Blanch, 2016, pág. 235.

14. Izquierdo Triana, H., «Inteligencia...», *op. cit.,* pág. 218.

15. Oliver Atenas, E., «Inteligencia...», *op. cit.,* pág. 237.

De este modo, como afirma Oliver Atenas, la inteligencia económica se encuentra vinculada con la estrategia y su puesta en acción, siendo el elemento esencial de la investigación e interpretación de las intenciones y capacidades de los competidores. Por tanto, constituye una herramienta esencial para garantizar la defensa de la posición actual del Estado o de la organización, así como un medio para obtener supremacía concreta de acuerdo con los intereses estratégicos[16]. En palabras de este autor, «*la inteligencia económica, por tanto, se apoya en la vigilancia del entorno competitivo, diferenciándose de otros procesos o sistemas de inteligencia en tres elementos principales:*

a) *sus fines son exclusivamente económicos;*

b) *trabaja con fuentes abiertas;*

c) *deber ser ética en todas sus acciones*»[17].

Así pues, la inteligencia económica se desliga totalmente de cualquier práctica que pudiese suponer la comisión de conductas ilícitas como el espionaje industrial[18]. Como afirman González Cussac y Larriba Hinojar, el espionaje económico e industrial ha de ser, y es, conforme a las diferentes legislaciones vigentes, una práctica prohibida en el ejercicio de la inteligencia económica y competitiva[19]. En el caso de España, el marco jurídico se articula fundamentalmente a través de las siguientes normas:

a) la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal;

b) la Ley 15/2007, de 3 de julio, de Defensa de la Competencia;

c) la Ley 3/1991, de 10 de enero, de Competencia Desleal.

En definitiva, como establecen Esteban Navarro y Carvalho, la inteligencia económica puede ser entendida como una inteligencia especializada que se ocupa de la obtención y el procesamiento de la información financiera, económica y empresarial de un Estado, para permitir una eficaz salvaguarda de los intereses nacionales tanto en el interior como en el exterior[20].

## 2.5. El Informe Draghi: ¿una última llamada?

El Informe «El futuro de la competitividad en Europa» —también conocido, por su autor, como el Informe Draghi—, presentado el 9 de septiembre de 2024 a petición de la Comisión Europea, constituye una nueva hoja de ruta

16. *Idem*., pág. 237.

17. *Ibid*., págs. 237-238.

18. Izquierdo Triana, H., «Inteligencia...», *op. cit.,* págs. 216-217.

19. González Cussac, J. L., Larriba Hinojar, B., *Inteligencia económica y competitiva*, Valencia, Tirant lo Blanch, 2011, pág. 53.

20. Esteban Navarro, M. A., Carvalho, A. V., «Inteligencia: concepto y práctica» en González Cussac, J. L. (coord.): *Inteligencia*, Valencia, Tirant lo Blanch, 2012, pág. 48.

para el futuro económico y estratégico de la UE —con más de 170 propuestas, no se limita a describir un diagnóstico—. Sin embargo, ahora corresponde a los Estados miembros aceptar reformas profundas, ceder competencias, coordinar políticas —no bloquearlas— y financiarlas adecuadamente. Y es que, como afirman Arnal, Feás, Otero Iglesias y Steinberg, *«el Informe Draghi no debería terminar en un cajón»*[21].

El documento consta de seis apartados: una descripción inicial de la situación actual; los tres principales desafíos (el cierre del *gap* de innovación respecto a Estados Unidos, cómo compatibilizar descarbonización y competitividad y cómo aumentar la seguridad económica y reducir las dependencias); y dos requisitos para lograrlo, que son un refuerzo de la inversión pública y privada y una mejora de la gobernanza europea (incluida la política de competencia)[22].

En este contexto, la reciente Brújula para la Competitividad —adoptada en 2025— se basa en las recomendaciones formuladas por Mario Draghi en su informe. El objetivo de la Brújula es facilitar y acelerar la actividad empresarial y asegurar la prosperidad de la UE. En particular, orienta el trabajo de la Comisión Europea para el período 2024-2029 sobre la base de tres pilares[23]:

a) subsanar el desfase en innovación con los principales competidores de la UE;

b) vincular descarbonización y competitividad;

c) reducir las dependencias y aumentar la seguridad.

Así pues, la propuesta de crear una División de Inteligencia Económica (*Economic Intelligence Division,* en adelante también EID por sus siglas en inglés) en el seno de la Comisión Europea se inserta plenamente en esta lógica. Un órgano de este tipo permitiría dotar a los comisarios de un análisis sistemático y anticipatorio sobre riesgos y oportunidades en el plano económico global, reforzando la capacidad de la UE para actuar de manera coherente con las propuestas formuladas en el Informe Draghi y con los compromisos asumidos en la Brújula para la Competitividad.

En otras palabras, la creación de la EID no solo constituiría una innovación en materia de inteligencia, sino también un paso necesario para avanzar en la ejecución efectiva de las recomendaciones presentadas, consolidando la competitividad como un elemento central en la UE. *«Durante los últimos 20 años, la productividad de Europa ha ido a la zaga de la de otras grandes economías. Es urgente actuar para reactivar la competitividad de*

21. Arnal, J., Feás, E., Otero Iglesias, M., Steinberg, F., El informe Draghi no debería terminar en un cajón. *Análisis del Real instituto Elcano*, núm. 120, 2024, pág. 1.

22. *Ibid*., págs. 1-2.

23. <https://www.consilium.europa.eu/es/policies/competitiveness-compass/#enablers> [última consulta: 17 de agosto de 2025].

*Europa»*[24]. ¿Una última llamada? *«El poder económico en declive de estos países indica que estamos ante el último hurra del viejo orden»* (Estados Unidos y la UE)[25].

## 3. Propuesta: una División de Inteligencia Económica

En palabras de Fernández Díaz, *«en el proceso de toma de decisiones, y la consiguiente aplicación y supervisión de las políticas públicas, cualquier decisor político necesita información y, en esto, la Unión Europea no es una excepción. Es decir, al igual que sucede a los gobiernos de los Estados miembros, todo el entramado institucional de la Unión Europea necesita estar suficientemente informado para tomar las decisiones adecuadas en todo momento»*[26]. Por su parte, Díaz-Caneja Greciano afirma que *«la UE, como organización supranacional necesita, igual que cualquier autoridad política, una información continuada, validada, integrada y oportuna, que apoye el proceso de decisiones»*[27].

La creación de una División de Inteligencia Económica en el seno de la Comisión Europea responde a una necesidad estructural de la UE: disponer de un mecanismo propio capaz de anticipar riesgos, identificar oportunidades y ofrecer un análisis estratégico integral en el ámbito económico. A diferencia de los actuales órganos fragmentados —que desarrollan trabajos sectoriales—, esta División podría completar el ciclo de inteligencia en su totalidad, lo que permitiría hablar de un verdadero sistema de inteligencia (económico) en sentido estricto y no únicamente de actividades analíticas o de intercambios de información.

La División de Inteligencia Económica (EID) se caracterizaría, además, por trabajar exclusivamente con fuentes abiertas, lo que garantizaría tanto su legitimidad como su compatibilidad con el marco jurídico de la UE. En este sentido, la producción de inteligencia económica no supondría una intromisión en las competencias de seguridad nacional reservadas a los Estados miembros conforme al art 4.2 TUE, ya que sus fines se circunscribirían a la esfera económica y estratégica, sin penetrar en ámbitos (sensibles) de defensa o seguridad interior.

El objetivo de la EID sería, por tanto, apoyar a la Comisión Europea en la toma de decisiones, reforzando la competitividad y la autonomía estratégica

24. <https://www.consilium.europa.eu/es/policies/competitiveness-compass/#enablers> [última consulta: 17 de agosto de 2025].

25. <https://www.washingtonpost.com/opinions/2022/04/25/is-this-the-western-alliances-last-hurrah-ukraine-russia/> [última consulta: 17 de agosto de 2025].

26. Fernández Díaz, C. A., Inteligencia y Seguridad desde el Derecho de la Unión Europea: cooperación e integración. *Revista del ejército de tierra español*, núm. 906, 2016, pág. 24.

27. Díaz-Caneja Greciano, J. M., La cooperación de inteligencia..., *op. cit.,* pág. 20.

de la Unión —sin menoscabar la soberanía nacional de los Estados miembros—. Respecto a su ubicación institucional, se considera adecuada situarla bajo la dependencia directa del Presidente y del Colegio de Comisarios.

Como se ha mencionado con anterioridad, un órgano con estas características proporcionaría a los comisarios una visión anticipatoria e integrada de los desafíos económicos globales, permitiendo orientar de manera más coherente las políticas de la UE. Además, reforzaría la capacidad de la Comisión Europea para cumplir con las propuestas formuladas en el Informe Draghi y con los compromisos asumidos en la Brújula para la Competitividad.

## 4. Propuesta alternativa: transformar el Joint Research Centre

La creación de una División de Inteligencia Económica en el seno de la Comisión Europea podría enfrentarse a resistencias políticas significativas. Los Estados miembros, debido a cuestiones de confianza[28], son reticentes a cualquier iniciativa que pueda interpretarse como una cesión de competencias —aunque en este caso no lo sea—. Incluso tratándose de inteligencia económica, es previsible que ciertos gobiernos perciban el establecimiento de un nuevo órgano como un primer paso hacia la conformación de una arquitectura europea de inteligencia común, ámbito en el que las reticencias siguen siendo muy fuertes.

Ante este escenario, una posible alternativa consistiría en reforzar y transformar el *Joint Research Centre* (en adelante JRC). El JRC es un centro que desempeña funciones de asesoramiento científico y técnico a la Comisión Europea, proporcionando la base científica para futuras iniciativas políticas, y que ayuda a los responsables políticos a monitorizar y evaluar el impacto de sus políticas[29].

En particular, el JRC organiza sus actividades en 25 carteras científicas que ofrecen una visión más profunda y apoyan las siete prioridades de la Comisión Europea para el período 2024-2029[30]:

a) Europa como continente de crecimiento económico, emprendimiento e innovación, garantizando la competitividad, la prosperidad y la equidad;

b) afrontar los retos de Europa en materia de seguridad y defensa y mejorar la preparación y la gestión de crisis;

---

28. Véase González López, D., La integración europea en materia de inteligencia..., *op. cit.,* págs. 10-11.

29. <https://commission.europa.eu/about/departments-and-executive-agencies/joint-research-centre_en> [última consulta: 17 de agosto de 2025].

30. <https://commission.europa.eu/priorities-2024-2029_en> [última consulta: 17 de agosto de 2025].

c) promover la justicia social, aumentar la solidaridad en nuestra sociedad y garantizar la igualdad de oportunidades para todos;

d) construir un sistema agrícola y alimentario competitivo y resiliente, salvaguardar la biodiversidad y prepararse para un clima cambiante;

e) situar a los ciudadanos en el centro de nuestra democracia para empoderar a todos y ayudar a dar forma al futuro de la UE;

f) centrarse en un vecindario más amplio para abordar los desafíos globales y promover la paz, las asociaciones y la estabilidad económica;

g) un presupuesto de la UE moderno y reforzado y una agenda de reformas ambiciosa para cumplir nuestros objetivos.

Si bien el JRC no elabora inteligencia —carece de las metodologías propias y se centra en la producción de conocimiento científico—, dispone de una estructura consolidada y una legitimidad institucional que podría facilitar su evolución hacia una unidad de inteligencia económica. La transformación consistiría:

a) crear una unidad de inteligencia dentro de la estructura del JRC[31];

b) dotarla de competencias específicas en materia de análisis económico, incorporando el ciclo de inteligencia;

c) integrar su labor en los procesos de toma de decisiones de la Comisión Europea;

d) asegurar su coherencia con los compromisos asumidos en la Brújula para la Competitividad.

Ahora bien, aunque la opción más adecuada es la creación de una División de Inteligencia Económica, la creación de una unidad de inteligencia en la estructura del JRC ofrece una vía intermedia — y más realista— capaz de superar las barreras políticas. Además, su adopción podría contribuir a generar un clima de mayor normalización institucional, allanando el camino hacia la futura consolidación de divisiones o centros de inteligencia en el ámbito de la Unión Europea.

## 5. Conclusiones

La creación de una División de Inteligencia Económica en el seno de la Comisión Europea permitiría la consecución de tres objetivos primordiales:

a) anticipar riesgos y oportunidades globales;

b) dotar a los comisarios de inteligencia estratégica integrada para la toma de decisiones —mejorando la calidad de estas—;

31. Independientemente de esta nueva unidad, el JRC seguiría ejerciendo sus funciones de asesoramiento científico y técnico.

c) consolidar la autonomía estratégica europea mediante un sistema propio de inteligencia económica —siguiendo el camino marcado por el Informe Draghi—.

Con todo, la paradoja resulta evidente. Si la inteligencia económica, concebida como una herramienta esencial orientada a *«fomentar la competitividad y proteger y aumentar la influencia del Estado y su estructura empresarial en el contexto internacional»*[32], se caracteriza por tener fines exclusivamente económicos, operar mediante fuentes abiertas y por requerir un estricto cumplimiento ético y de la legalidad, difícilmente podría considerarse contraria al art. 4.2 TUE —que reserva la seguridad nacional cómo una competencia exclusiva de cada Estado miembro—.

En consecuencia, cabe preguntarse por qué la UE, que debería aspirar a competir con potencias mundiales como Estados Unidos o China —países que evidentemente cuentan con la inteligencia proporcionada por sus servicios de inteligencia nacionales—, continua en desventaja.

La ausencia de una División de Inteligencia Económica en el seno de la Comisión Europea no parece responder a un impedimento jurídico (competencial), sino más bien a resiliencias políticas y estratégicas. Quizás la respuesta resida en la presión indirecta ejercida por terceros países, a quienes no les interesa una UE más autónoma y cohesionada en el plano geoeconómico.

## BIBLIOGRAFÍA

**Arnal, J.**, **Feás, E.**, **Otero Iglesias, M.**, **Steinberg, F.**, El informe Draghi no debería terminar en un cajón. *Análisis del Real instituto Elcano*, núm. 120, 2024.

**De Castro García, A.**, «Ciclo de inteligencia» en Díaz Fernández, A. M. (dir.): *Conceptos fundamentales de inteligencia*, Valencia, Tirant lo Blanch.

**Díaz-Caneja Greciano, J. M.**: La cooperación de inteligencia en la Unión Europea. *Boletín Instituto Español de Estudios Estratégicos*, núm. 6, 2014.

**Esteban Navarro, M. A.**, **Carvalho, A. V.**, «Inteligencia: concepto y práctica» en González Cussac, J. L. (coord.): *Inteligencia*, Valencia, Tirant lo Blanch, 2012.

**Fernández Díaz, C. A.**, Inteligencia y Seguridad desde el Derecho de la Unión Europea: cooperación e integración*. Revista del ejército de tierra español*, núm. 906, 2016.

**González Cussac, J. L.**, **Larriba Hinojar, B.**, *Inteligencia económica y competitiva*, Valencia, Tirant lo Blanch, 2011.

32. Oliver Atenas, E., «Inteligencia...», *op. cit.*, p. 238.

**González López, D.**, La integración europea en materia de inteligencia: ¿un servicio de inteligencia europeo? *Studia Humanitatis Journal*, vol. 4, núm. 2, 2024.

**Izquierdo Triana, H.**, «Inteligencia competitiva» en Díaz Fernández, A. M. (dir.): *Conceptos fundamentales de inteligencia*, Valencia, Tirant lo Blanch, 2016.

**López Canorea, A.**, **Marrades, A.**, **González Márquez, J.**, *La pugna por el nuevo orden internacional. Claves para entender la geopolítica de las grandes potencias*, Barcelona, Espasa, 2023.

**Oliver Atenas, E.**, «Inteligencia económica» en Díaz Fernández, A. M. (dir.): *Conceptos fundamentales de inteligencia*, Valencia, Tirant lo Blanch, 2016.

**Sahagún, F.**, «¿Declive o recomposición de Occidente? en Beneyto, J. M. (dir.): *¿Hacia un nuevo orden mundial? La guerra de Ucrania y sus consecuencias*, Barcelona, Deusto.

**Wilensky, H.**, *Organizational Intelligence: Knowledge and Policy in Government and Industry,* 1967.

# DESAFÍOS POLÍTICOS Y JURÍDICOS PARA UNA COMUNIDAD DE INTELIGENCIA EUROPEA: ENTRE SEGURIDAD Y PROTECCIÓN DE DATOS

**Irene Gil Matos**

*Máster Universitario en Derecho Internacional*
*Universidad Complutense de Madrid*

## 1. Introducción

El contexto internacional contemporáneo se caracteriza por su dinamismo e interdependencia. En este escenario las amenazas se vuelven cada vez más complejas y multidimensionales, lo que hace que garantizar la seguridad dependa de un flujo constante de información para ofrecer respuestas rápidas y efectivas.

De tal forma, la información no solo juega un papel fundamental en el mundo actual, sino que se ha consolidado como fuerza revolucionaria, conduciendo a un cambio en las propias relaciones de interdependencia[1]. Por esta razón, la capacidad de información se configura como un recurso de poder determinante dentro de las relaciones internacionales[2].

Partiendo de esta premisa, formulada en su momento por Joseph S. Nye y Robert. O. Keohane, la relevancia de un actor internacional no dependerá únicamente de sus recursos materiales, sino que estará condicionada por su capacidad para gestionar y utilizar el creciente tráfico de información. En esta tesitura, resulta decisivo un procesamiento eficiente de dicha información que sea capaz de generar conocimiento útil para la toma de decisiones.

Ante este escenario global, la Unión Europea se erige como una entidad política que numerosos autores definen como *sui generis*. El proyecto europeo se presenta como una idea federal utópica, que trasciende la mera coo-

1. Keohane, R., Nye, J., *Power and Interdependence*, 4ª ed., Lognman, 1997, pág. 215.

2. *Ibid.,* pág. 217.

peración interestatal y permanece en constante trasformación. Esta visión ha sido el impulso que permitió la construcción del actor global, normativo y diplomático que es hoy en día, un actor que se consolida progresivamente como entidad autónoma con creciente influencia internacional[3]. Ahora bien, a pesar de ello, no deja de ser una organización internacional cuya personalidad jurídica es derivada y, por tanto, se encuentra limitada a la voluntad soberana de sus integrantes. Esta condición implica una dependencia que condiciona el progreso de la integración política.

En este sentido, uno de los ámbitos que permanece íntegramente bajo la soberanía de los Estados miembros es la seguridad nacional, que incluye el funcionamiento de los servicios de inteligencia encargados de recopilar y procesar información. En cualquier caso, ante las necesidades anteriormente expuestas, surge la creciente preocupación por coordinar de manera efectiva los esfuerzos nacionales para poder ofrecer respuestas más eficaces ante las nuevas amenazas. Y es en este contexto donde cobra fuerza la idea de crear una Comunidad de Inteligencia Europea, capaz de dotar a la Unión Europea (UE) de los medios necesarios para desempeñar sus cada vez mayores funciones atribuidas.

Bajo este planteamiento, se manifiesta la necesidad de construir confianza mutua para lograr la seguridad colectiva. En la actualidad, persiste una desconfianza entre Estados miembros que dificulta los intercambios de información y la cooperación entre servicios de inteligencia[4]. Esto limita no solo las capacidades de la propia UE, sino el potencial que ofrece para la seguridad nacional de los países europeos. Dicha brecha se origina, en gran medida, en las diferencias entre culturas operativas, capacidades técnicas y marcos legales, lo que complica la colaboración en un terreno tan sensible como es el tratamiento de la información.

A este respecto, los escándalos de espionaje acontecidos en las últimas décadas han puesto de relieve la necesidad de que todos los Estados miembros sean capaces de ofrecer garantías equivalentes y alineadas con los valores europeos en materia de protección de datos, incluyendo las prácticas de las agencias de seguridad. Después de todo, la confianza no puede asumirse como un hecho dado, sino que debe ser el resultado de un proceso continuo del cual surgen proyectos como la propia Unión Europea.

Por estos motivos, el siguiente análisis se centra en los principales retos para llegar a construir una Comunidad de Inteligencia, con especial atención a las preocupaciones crecientes en lo relativo a la protección de datos y la seguridad nacional.

---

3. Véase Aldecoa, F. y García Cancela, E., *La Unión Europea: De la idea utópica de Europa a la Unión Europea como potencia mundial*, Shackleton, 2023.

4. González López, D., «La integración europea en materia de inteligencia: ¿un servicio de inteligencia europeo?», en *Studia Humanitatis Journal*, vol. 4(2), 2024, págs.10-11.

## 2. Marco jurídico general de la seguridad y la protección de datos en la unión europea

Para abordar esta cuestión hay que empezar por delimitar el marco jurídico en el que se enmarcan tanto la seguridad como la protección de datos dentro del Derecho de la Unión Europea. Por tanto, tratar este asunto nos remite a las disposiciones del derecho originario tal y como fueron reformuladas por el Tratado de Lisboa.

En primer lugar, en lo que respecta al asunto de la seguridad, en este contexto se pueden tener en cuenta dos vertientes en las que la información juega un papel clave para el funcionamiento y desarrollo de las actividades. La primera de ellas se refiere al Espacio de Libertad, Seguridad y Justicia (ELSJ). La segunda la constituye la propia seguridad de la Unión Europea como sujeto autónomo, es decir, la Política Exterior y de Seguridad Común (PESC).

Por la propia estructura de la organización, el reparto de competencias se encuentra en el núcleo de la discusión. Debido a ello, debe tenerse en cuenta al hablar de las posibilidades de su futuro desarrollo, ya que estas delimitan la capacidad de la UE para intervenir.

De esta manera, la seguridad nacional se contempla como una competencia exclusiva de cada Estado miembro[5]. Sin embargo y pese a esta disposición, el Espacio de Libertad, Seguridad y Justica se circunscribe dentro de las competencias compartidas entre los Estados miembros y la UE[6]. El objetivo de este es ofrecer un espacio sin fronteras interiores que sea capaz de garantizar la libre circulación de los ciudadanos europeos[7]. Dicho en otros términos, se trata de la construcción de un orden público europeo entendido por la Comisión Europea como el espacio que deriva de nuestras tradiciones democráticas y lo que entendemos por Estado de Derecho[8]. Sin embargo, también cuenta con una excepción de seguridad nacional, por la que las competencias de la UE no deben afectar al ejercicio de las responsabilidades de los Estados miembros sobre el mantenimiento de la ley y el orden para salvaguardar la seguridad interna[9].

Asimismo, el preámbulo del Tratado de la Unión Europea refleja claramente la intención de desarrollar la PESC para reforzar la identidad e independen-

5. Art. 4 (2) del Tratado de la Unión Europea (TUE), firmado el 13 de diciembre de 2007, Lisboa (Portugal).

6. Art. 4 (2) letra j) del Tratado de Funcionamiento de la Unión Europea, firmado el 13 de diciembre de 2007, Lisboa (Portugal).

7. Art. 3 (2) del TUE.

8. Coutts, S. D., «The Lisbon Treaty and the Area of Freedom, Security and Justice as an area of legal integration», en *Croatian Yearbook of European Law and Policy*, vol. 7, 2021, pág. 93.

9. Art. 72 del TFUE.

cia europeas. Con ello marca un objetivo central para el proyecto europeo de integración, que funciona en base a la solidaridad política mutua y la identificación de intereses generales[10]. De igual manera, una de sus intenciones manifiestas es la del fortalecimiento de la cooperación sistemática entre sus miembros[11].

Ahora bien, en la práctica estas disposiciones se encuentran con la soberanía nacional, siendo la seguridad y la defensa uno de los asuntos clásicos dentro de las teorías de construcción del Estado[12]. Desde la perspectiva de la construcción del Estado moderno, tanto la seguridad colectiva como la integración de mercados han sido lógicas presentes para la concentración de la autoridad política[13]. No obstante, en el proyecto europeo ha predominado esta última, erigiéndose sobre las bases de la legalidad y no sobre sus capacidades coercitivas[14]. Esto, sumado a que la UE es una organización internacional y no un Estado, deriva en la conclusión de que solo puede actuar dentro del limitado marco de las competencias otorgadas[15].

Sin embargo, esto no ha sido un óbice para poner en marcha distintas iniciativas cuando ha sido necesario. Así, cabe destacar que en los Tratados también se incluyen formas específicas de cooperación intergubernamental. Ejemplo de ello es la posibilidad que ofrecen de organizar bajo su responsabilidad la cooperación y coordinación entre servicios administrativos responsables de la seguridad nacional, un aspecto central dentro de este análisis[16]. También existen otras formas muy conocidas, como la Cooperación Estructurada Permanente (CEP)[17] o el Comité Permanente de Seguridad Interior (COSI)[18].

Dicho lo cual, algo que caracteriza a la UE es precisamente que se trata de un proyecto en desarrollo, que basa su evolución en la voluntad política de sus integrantes y sus necesidades dentro la Comunidad Internacional. Por ello, conviene señalar el papel central de la confianza en los marcos legislati-

10. Art. 24 (3) del TUE.

11. Art. 25 letra c) del TUE.

12. Véase Tilly, C., *Coerción, capital y los Estados europeos: 990-1990*, Basil Blackwell, Cambridge, 1990; o Buzan, B., *People, state and fear: an agenda for international security studies in the post-Cold War era*, 2ª ed., New York, Harvester Wheatsheaf, 1991.

13. Kelemen, R. D., Mcnamara K. R., «State-building and the European Union: Markets, War, and Europe's Uneven Political Development», en *Comparative Political Studies*, vol. 55(6), 2022, pág. 954.

14. *Ibid.*, pág. 981.

15. Craig, P., De Búrca, G., «Competence», en *EU Law: text, cases and materials*, 7ª ed., Oxford, Oxford University Press, 2008, pág. 103.

16. Art. 73 del TFUE.

17. Arts. 42 y 46 del TUE y Protocolo nº 10 sobre la Cooperación Estructurada Permanente establecida por el Artículo 42 del Tratado de la Unión Europea.

18. Art. 71 del TFUE.

vos nacionales, que puede ser muy relevante para profundizar la cooperación en determinadas materias. Tal es el caso de la protección de datos.

En este sentido, a nivel europeo se ha mostrado una gran preocupación por la regulación de este ámbito. Tanto es así que es recogido como un derecho fundamental en la propia Carta de los Derechos Fundamentales de la Unión Europea (CDFUE)[19]. Cabe destacar que esta tiene, además, el mismo valor jurídico que los propios Tratados constituyentes[20]. De la misma manera, el TFUE establece el derecho de toda persona a la protección de datos de carácter personal y al desarrollo de legislación del Parlamento Europeo para protegerlo[21]. De este artículo se excluye explícitamente el ámbito de la PESC donde, por las características previamente explicadas, queda regulado por el Consejo de la Unión Europea[22]. A este respecto, y para precisar lo anterior, también hay que añadir la disposición relativa a la cooperación en materia penal, donde el tratamiento de datos se regula mediante procedimiento legislativo ordinario[23].

Otro aspecto a considerar es la adhesión de la propia UE al Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales, que contiene a su vez el derecho al respeto de la vida privada y familiar[24].

El avance normativo en este aspecto lleva a considerarlo como un derecho derivado del cambio en el contexto social, y desarrollado en el momento presente por medio de la legislación secundaria de la Unión Europea[25]. En otras palabras, es una forma de derecho que funciona para mitigar las consecuencias de la incertidumbre provocada por el cambio social y asegurar el funcionamiento de un catálogo de derechos sustantivos constitucionales mediante la provisión de una infraestructura legal[26]. El marco actual se planteará más adelante, subrayando el vacío existente en cuanto a la armonización normativa en el campo de la seguridad y la protección de datos.

Por el momento, este apartado sirve para contextualizar tanto la protección de datos como de la seguridad en líneas generales, para posterior-

19. Art. 8 de la Carta de los Derechos Fundamentales de la Unión Europea, de 7 de diciembre de 2000, Niza (Francia).

20. Art. 6 del TUE.

21. Art. 16 del TFUE.

22. Art. 39 del TUE.

23. Art. 87 del TFUE.

24. Art. 8 del Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales, firmado el 4 de noviembre de 1950, Roma (Italia).

25. Hallinan, D., «A Theory of EU Data Protection Law», en *European Data Protection Law Review*, vol. 9(3), 2023, pág. 331.

26. *Ibid.,* pág. 311.

mente poder profundizar sobre sus límites y posibilidades. De esta forma, el siguiente punto que se debe abordar es la cooperación europea en materia de seguridad para proyectar la imagen fragmentada que existe en la actualidad.

## 3. Desarrollo y actualidad de las dinámicas de cooperación europeas

Tomando en consideración este marco preliminar, cabe destacar la propia evolución de la Unión Europea hacia el sujeto complejo que es hoy en día. Así, se observa que desde principios de los años 1990 la orientación económica de la integración europea ha sido superada por la racionalidad de la seguridad[27].

Para ello, conviene recapitular sobre las diversas iniciativas que han dado lugar a lo que se puede denominar arquitectura de seguridad europea, si bien esta no tiene una definición consensuada[28]. Aunque en un principio la seguridad no era destacada en la agenda comunitaria, las deficiencias en materia de cooperación en la lucha contra el crimen pusieron de manifiesto que este aspecto, en efecto, afectaba al funcionamiento de su economía. Este motivo llevó al proyecto funcionalista a apoyarse en estructuras como el Grupo TREVI, el Club de Berna o el Grupo Kilowatt[29].

Seguidamente, en los años 80 la integración europea fue profundizada gracias al Acuerdo de Implementación de Schengen y, especialmente, al Acta Única Europea. Esta, aunque se establecía sobre las bases de la cooperación intergubernamental, ya reconocía la libre circulación de personas como materia de competencia europea al incluirla dentro del mercado interior[30]. Esto requiere compartir información entre los Estados miembros para su funcionamiento.

Años después, el Tratado de Maastricht conformó la Unión Europea entorno a tres pilares esenciales, comenzando así un proceso de configuración constitucional que llevó al Tratado de Lisboa, donde ya se le otorgaba su personalidad jurídica propia[31]. Los antiguos pilares de Maastricht sentaron

27. Lavenex, S., Wagner, W., «Which European Public Order? Sources of Imbalance in the European Area of Freedom, Security and Justice», en European Security, vol. 16(3), 2007, pág. 239.

28. Angheland, S., Damen, M., *The future European security architecture: dilemmas for EU strategic autonomy*, European Parliamentary Research Service, 2025, pág. 1.

29. Díaz Fernández, A. M., «Evolución de la cooperación europea en inteligencia», en *Varia Historia*, vol. 28(47), 2012, pág. 164-166.

30. Art. 8 A del Acta Única Europea, firmada el 17 de febrero de 1986, La Haya (Países Bajos).

31. Art. 47 del TUE.

las bases tanto de la PESC como de la Justicia y Asuntos de Interior (JAI). Tras ello, en la Declaración Saint-Malo se destacó la importancia de que la UE contase con recursos de inteligencia propios para desarrollar la PESC, siendo reiterado seguidamente en la Declaración de Colonia[32].

Sin embargo, el punto de inflexión más evidente se dio a raíz de los atentados del 11 de septiembre de 2001 y los que posteriormente tuvieron lugar en suelo europeo. Además de expresar su apoyo de forma inmediata a Estados Unidos, la Unión Europea planteó una revisión profunda en materia de seguridad y crimen. De esta forma, tras el Consejo de Laeken de ese mismo año se implementaron medidas como la Orden Europea de Detención o las Decisiones Marco sobre la definición y lucha contra el terrorismo[33]. Por otro lado, los atentados de Madrid y Londres impulsaron la aceleración de la cooperación en la lucha contra el terrorismo mediante marcos legales y técnicos. Esto resultó en el Programa de Estocolmo, mediante el que se planteaba la reforma del intercambio de información centrado en la interoperabilidad y el desarrollo operativo[34].

Tras el Tratado de Lisboa se planteó un nuevo marco, que ya ha sido detallado en el apartado previo y que persiste en la actualidad. En virtud del cual conviven varias estructuras de seguridad. En 2010 se creó el COSI, que coordina agencias europeas como Europol, Eurojust, FRONTEX o CEPOL[35]. Además, en lo concerniente al ELSJ también conviene tener en mente el Sistema de Información Schengen (SIS II), el Sistema de Información de Aduanas (SIA), la Red Judicial Europea (RJE) y la Oficina Europea contra el Fraude (OEF). Asimismo, en el ámbito de la PESC destacan el Centro de Satélites de Torrejón (SatCen), el Instituto de Estudios de Seguridad (IES) y, sobre todo, el Centro de Inteligencia de la Unión Europea (EU INTCEN)[36].

Como se puede comprobar, la evolución del proyecto europeo ha transcendido el ámbito económico y político en base a las necesidades de seguridad. Con ello, la coyuntura internacional actual ha puesto de manifiesto la necesidad de un intercambio eficaz de información, un pensamiento que lleva presente prácticamente desde los inicios de la organización. En esta tesitura, en la que las nuevas amenazas se caracterizan por su multidimensionalidad y donde destacan las amenazas híbridas[37], un uso adecuado de la información resulta fundamental.

---

32. Díaz-Canaleja Greciano, J. M., *La cooperación de inteligencia en la Unión Europea*, Instituto Español de Estudios Estratégicos, Madrid, 2014, pág. 5.

33. Díaz Fernández, A. M., «Evolución...*op.cit.*, pág. 170.

34. *Ibid.,* pág. 182.

35. *Ibid.,* pág. 183.

36. Díaz-Canaleja Greciano, J. M., *La cooperación...*, *op.cit.*, pág. 8.

37. Véase Lonardo, L., «EU Law against hybrid threats: a first assessment», en *European Papers*, vol. 6(2), 2021, págs. 1075-1096.

Los servicios europeos de seguridad han tenido un gran desarrollo. No obstante, las deficiencias de este sistema siguen siendo destacadas y el cambio requiere de compromiso. Aunque la UE reitera la necesidad de mejorar la integración e interoperabilidad de los sistemas de información[38], sigue existiendo una clara fragmentación de los organismos y una marcada dependencia por parte de estos de los servicios nacionales. Pese a ello, la idea de una Agencia Europea sigue obstaculizada por la desconfianza[39] y por el riesgo de duplicar de capacidades y esfuerzos innecesariamente[40]. En la actualidad, INTCEN es la agencia con más potencial para aunar los esfuerzos y liderar la transformación, pero continua con un mandato limitado a la inteligencia de fuente abierta y la información proporcionada por los Estados miembros voluntariamente[41].

Con todo, el tema planteado en el párrafo anterior es demasiado amplio para la proposición aquí defendida. A este respecto, dicha apreciación se refiere y limita al tratamiento de la información para la seguridad europea, un asunto ligado a la protección de datos. Pese a la extensa normativa europea sobre protección de datos, la competencia soberana en materia de seguridad hace que los servicios de inteligencia y seguridad de los Estados estén regulados por sus propias leyes nacionales.

Así, los escándalos de vigilancia masiva han puesto de manifiesto la necesidad de una transparencia y una supervisión equitativas. Para ello, unas garantías equivalentes a nivel nacional podrían ser una precondición necesaria para poder derivar mayores competencias a las instituciones europeas en materia de datos para su uso en el ámbito de la seguridad.

Por consiguiente, una vez detallado el escenario legal, político y técnico en el que se encuentra este asunto, queda por entender la interacción entre estos marcos y el vacío de protección de datos al que dan lugar.

## 4. La tensión entre la seguridad y la protección de derechos humanos

Este apartado parte del supuesto básico de que en toda situación que implique uso de información personal y seguridad nacional siempre existirá

38. Gutheil, M. et al, *Study on Interoperability of Justice and Home Affairs Information Systems*, Policy Department for Citizens' Rights and Constitutional Affairs of the European Parliament, Bruselas, 2018, pág. 83.

39. Protopapas, G. X., «European Union's Intelligence Cooperation: A Failed Imagination?», en *Journal of Mediterranean and Balkan Intelligence*, vol. 4(2), 2014, pág. 50.

40. Díaz-Canaleja Greciano, J. M., *La cooperación...*, *op.cit.*, pág. 23.

41. Nomikos, J. M., «European Union Intelligence Analysis Centre (INTCEN): Next stop to an Agency?», en *Journal of Mediterranean and Balkan Intelligence*, vol. 4(2), 2014, pág. 8.

una tensión entre el interés público y los derechos individuales. El ejemplo de las medidas preventivas de la Unión Europea para anticipar riesgos y amenazas pone de manifiesto la necesidad de estar alerta ante su posible efecto erosivo para los derechos humanos[42].

En conformidad, el derecho a la protección de datos, como se ha visto, es un derecho fundamental de la Unión Europea. Sin embargo, el propio Reglamento General de Protección de Datos (RGPD) establece que este no es un derecho absoluto, sino que debe ser considerado por su función en la sociedad y en equilibrio con otros derechos fundamentales, con arreglo al principio de proporcionalidad[43]. En cualquier caso, la organización internacional le da gran importancia, y es por ello por lo que ha desarrollado varios instrumentos legales para su protección de forma uniforme en todos los Estados miembros.

Ahora bien, el marco europeo de protección de datos también se encuentra fragmentado y desagregado. El más completo es el ya mencionado RGPD, cuyo ámbito de aplicación material son los datos de carácter personal. No obstante, excluye cualquier actividad no comprendida en el Derecho de la Unión; las actividades PESC de los Estados miembros; las actividades de las personas físicas exclusivamente personales o domésticas; y las actividades de las autoridades competentes con fines de prevención, investigación, detección o enjuiciamiento por infracciones legales, y ejecución de sanciones penales[44].

Por otro lado, algunos instrumentos europeos tienen como objeto un sector específico. Entre ellos se encuentran la Directiva (UE) 2016/680, que se refiere a la última exclusión del RGPD. Es decir, esta establece un estándar mínimo de garantías para el tratamiento de datos de carácter personal por parte de las autoridades competentes en el ejercicio de actividades comprendidas en el ámbito de aplicación del Derecho de la Unión[45].

Por su parte, el Reglamento (UE) 2018/1725 se encarga de la regulación del tratamiento de datos personales por todas las instituciones y órganos de la

42. Den Boer, M., «Juggling the Balance between Preventive Security and Human Rights in Europe», en *Security and Human Rights*, vol. 26(2-4), 2015, pág. 127.

43. Strmečki, S., Pejaković-Đipi, S., «Data Protection, Privacy and Security in the context of artificial intelligence and Conventional Methods for Law Enforcement», en *EU And Comparative Law Issues and Challenges Series*, vol. 7, 2023, pág. 572.

44. Art. 2 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de esos datos.

45. Arts. 1 y 2 de la Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos.

Unión, excluyendo los datos personales operativos por parte de Europol, que se regulan por el Reglamento (UE) 2016/794[46].

En esta línea también existía una propuesta de Reglamento para actualizar la Directiva 2002/58/EC, sobre la confidencialidad de las comunicaciones electrónicas. Sin embargo, la propuesta ha quedado obsoleta debido a los retrasos sufridos por las negociaciones[47], por lo que finalmente fue retirada en febrero de 2025. Así, la Directiva vigente solo se aplica a las actividades dentro del Derecho de la Unión, excluyendo explícitamente la seguridad pública, la defensa y la seguridad del Estado[48].

Ante esta situación se puede observar cómo el marco legal no solo se encuentra fragmentado, sino que excluye de su ámbito de aplicación los servicios de seguridad nacionales. No obstante, esto no quiere decir que sea un debate reservado a la esfera nacional. De hecho, son precisamente los escándalos de espionaje y vigilancia masiva a nivel internacional los que han avivado esta discusión, una cuestión que ya ha sido tratada por tribunales internacionales.

Las filtraciones de Edward Snowden supusieron un punto de inflexión para esta controversia. Este caso evidenció el riesgo de vigilancia masiva por parte de las agencias de seguridad nacionales, además de revelar la colaboración entre actores públicos y privados en distintos países[49].

A este respecto, los jueces del Tribunal de Justicia de la Unión Europea (TJUE), aunque no hayan establecido una prohibición expresa para la retención de datos dentro de la seguridad nacional, han tratado de limitar la retención masiva de datos incluyendo este aspecto de la soberanía[50]. Con ello, y pese a las limitaciones, el TJUE ha determinado que los Estados miembros no pueden desligarse de sus obligaciones respecto a los derechos humanos bajo el Derecho de la Unión[51].

---

46. Art. 2 del Reglamento (UE) 2018/1725 del Parlamento Europeo y del Consejo de 23 de octubre de 2018 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones, órganos y organismos de la Unión, y a la libre circulación de esos datos.

47. Celeste, E., Formici, G., «Constitutionalizing Mass Surveillance in the EU: Civil Society Demands, Judicial Activism, and Legislative Inertia», en *German Law Journal*, vol. 25, 2024, pág. 444.

48. Art. 1 de la Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas).

49. Véase Lyon, D., «Surveillance, Snowden, and Big Data: Capacities, consequences, critique», en *Big Data & Society*, vol. 1(2), 2014, págs.1-13.

50. Celeste, E., Formici, G., «Constitutionalizing... *op.cit*., pág. 445.

51. Mitsilegas, V. et al, «Data retention and the future of large-scale surveillance: The evolution and contestation of judicial benchmarks», en *European Law Journal*, vol. 29(1-2), 2023, pág. 210.

Estas conclusiones emanan de pronunciamientos por parte de este tribunal, aunque casos similares también han sido sometidos al Tribunal Europeo de Derechos Humanos (TEDH). Entre la jurisprudencia más significativa del TJUE se encuentran los asuntos Digital Rights Ireland, Schrems y Tele2/Watson. Si bien las repercusiones del primero no estuvieron claras, Schrems determinó que la trasferencia de datos con terceros estados solo debía darse si estos ofrecían estándares de protección equivalentes a los de la UE[52]. Por su parte, el caso de Tele2/Watson tuvo mayor impacto, llegando a afirmar que las salvaguardas relativas a la protección de datos son en todo caso un asunto concerniente al Derecho de la Unión[53]. Mediante esta última sentencia, el TJUE determinó que la retención general e indiscriminada de datos no era compatible con la CDFUE[54].

Estas sentencias cristalizan las opiniones y preocupaciones de la sociedad civil en su conjunto, a las que se suman jueces nacionales y la academia. En consecuencia, evidencian la concienciación social respecto de la intromisión y el impacto que esta genera, no solo para sus derechos, sino en el vínculo que los ciudadanos mantienen con los poderes públicos[55].

En definitiva, lo que el TJUE ha puesto de manifiesto es que las disposiciones relativas a la retención y al acceso a los datos de comunicaciones conservados con fines de seguridad se encuentran dentro del ámbito de aplicación del Derecho de la Unión[56]. Esto plantea no solo la necesidad de armonizar las legislaciones nacionales entre los distintos Estados europeos, sino una estandarización entorno a los principios del ordenamiento jurídico europeo. Y ya no solo a nivel estatal, sino dentro de las propias agencias, aunque estén dentro del Derecho de la Unión, que también cuentan con diferentes políticas y regímenes de cumplimiento en materia de derechos humanos[57].

Consecuentemente, este apartado recapitula sobre las condiciones de la protección de datos a nivel europeo y cómo estas disposiciones excluyen deliberadamente la seguridad nacional. No obstante, también se señala la forma en que el TJUE ha podido conocer sobre la cuestión y sentar jurisprudencia al respecto.

Por lo tanto, si lo que se plantea es la posibilidad de crear una Comunidad de Inteligencia a nivel europeo, esta debe construirse sobre los valores europeos. Este planteamiento requiere de la existencia de marcos legales claros y de mecanismos de supervisión efectivos a nivel nacional. Sin embargo, como

52. Cameron, I., «European Union Law Restraints on Intelligence Activities», en *International Journal of Intelligence and Counterintelligence*, vol. 33, 2020, pág. 456.

53. *Ibid.,* pág. 457.

54. *Idem*.

55. Celeste, E., Formici, G., «Constitutionalizing...*op.cit.,* pág. 437.

56. *Ibid.,* pág. 445,

57. Den Boer, M., «Juggling the... *op.cit.*, pág. 139.

se detallará en el siguiente apartado, esto supone solamente una precondición que debe ir acompañada de otras reformas dentro del escenario europeo actual.

## 5. Obstáculos para una comunidad de inteligencia integrada

A lo largo de la exposición de esta propuesta se ha detallado de manera concisa la situación de la seguridad y la protección de datos en la Unión Europea, así como sus avances y limitaciones. Siguiendo este enfoque, en esta sección se abordarán los principales obstáculos que condicionan el desarrollo de una Comunidad de Inteligencia unificada, de forma que se pueda obtener una visión completa de la situación vigente.

De forma general, Eveline R. Hertzberger destaca cuatro problemas centrales[58]:

a) La falta de voluntad por parte de las agencias de inteligencia y servicios de seguridad nacionales para compartir información.

b) La desconfianza entre agencias de inteligencia nacionales.

c) Las diferencias de organización entre las estructuras de las agencias nacionales de los Estados miembros.

d) Las estrictas normas de protección de datos.

De ellas derivan las cuestiones esenciales que han guiado este análisis. Partiendo de ellas, las limitaciones sustanciales se deben a una arquitectura fragmentada, que puede llevar a la duplicación de esfuerzos por la falta de interoperabilidad entre estructuras. Es decir, aunque si que existan instituciones de inteligencia, falta una agencia centralizada e institucionalizada con un mandato delimitado de forma precisa[59].

Ante este escenario, la seguridad nacional sigue siendo una competencia exclusiva de los Estados miembros, lo que dificulta la coordinación de iniciativas comunes que afecten a este ámbito. En consecuencia, la información que llega a agencias como Europol es reducida, obedeciendo a diversos factores. Entre ellos, destaca la defensa de la soberanía, reforzada por la cultura de secretismo y la marcada autonomía de los servicios nacionales[60].

Sin embargo, en el escenario internacional actual, incluso los países miembros preeminentes son demasiado pequeños para desarrollar la inteligencia

58. Protopapas, G. X., «European...*opt.cit.*, pág. 52.

59. *Ibid.,* pág. 55.

60. Bureš, O., «Intelligence sharing and the fight against terrorism in the EU: lessons learned from Europol», en *European View*, vol. 15, 2016, pág. 62.

global que se necesita. Por esta misma razón, la cooperación entre servicios es indispensable para que la Unión Europea disponga del instrumento de inteligencia adecuado[61].

En este sentido, lo que se necesita no es la creación de nuevas estructuras, sino la remodelación de las existentes, apoyadas por unas políticas sólidas y con permanencia en el tiempo[62]. La creación de una Comunidad de Inteligencia no viene precedida por la existencia de una Agencia en sí misma, sino por la concertación de intereses comunes y la movilización de recursos entorno a ellos. Y es que, al fin y al cabo, aunque los países europeos compartan principios y valores, no siempre comparten opiniones, intereses o preocupaciones[63].

Por consiguiente, las diferentes culturas operativas y marcos legales de las agencias nacionales complican la transmisión de la información a nivel europeo. En última instancia, esto repercute en la toma de decisiones en la Unión Europea, ya que uno de los principales problemas detectados en este proceso es la escasa información e inteligencia disponible[64].

Por esta misma razón, resulta imprescindible que se genere la confianza requerida para poner en común una atribución estatal tan delicada como la información recabada por sus servicios. Con tal fin, es fundamental el compromiso de los Estados con la protección de datos que demuestre su ineludible responsabilidad bajo los estándares europeos. En consecuencia, esto se traduce en la necesidad de que los Estados miembros recuerden las líneas de intereses en común que conducen la integración europea[65].

Asimismo, conviene enfatizar uno de los mayores retos pendientes, que es determinar cómo avanzar en la cooperación sin que afecte a las actividades de los servicios de seguridad nacionales. Es fundamental que cualquier iniciativa respete la autonomía de estos servicios, evitando con ello que se vea comprometida su capacidad de actuación.

La creación de una Comunidad de Inteligencia Europea no implica la sustitución de estos servicios, sino la consolidación de un marco institucional para el intercambio eficiente y seguro de información. Para ello, debe estar fundamentado sobre la confianza, la eficiencia y los principios democráticos que rigen el proyecto europeo. De esta manera no debilitará, sino que reforzará las capacidades nacionales expandiendo con ello su alcance.

---

61. Palacios, J. M., «Cooperación entre servicios de inteligencia: la dimensión regional», en *Revista de Relaciones Internacionales, Estrategia y Seguridad*, vol. 16(1), 2021, pág. 23.

62. Díaz-Caneleja Greciano, J. M., *La cooperación…op.cit.,* pág.4.

63. González López, D., «La integración europea…*op.cit.,* pág. 17.

64 *Ibid.,* pág. 3.

65. González García, A., «Condiciones de viabilidad para establecer un Sistema Integrado de Inteligencia Europeo», en *Grupo de Estudios en Seguridad Internacional*, vol. 9, 2018.

En resumidas cuentas, al igual que la propia Unión Europea, la Comunidad de Inteligencia es un proyecto en desarrollo que en la actualidad se encuentra sometido a debates y ajustes. Los próximos pasos deben ir dirigidos a fomentar la confianza en los marcos legales y técnicos de los Estados miembros y de las propias instituciones europeas. A partir de esta lógica, en el largo plazo se podría vislumbrar una arquitectura institucional europea que sea capaz de desarrollar el llamado ciclo de la inteligencia de forma autónoma.

## 6. Conclusiones

Tras esta valoración, centrada en la seguridad y la protección de datos en la Unión Europea, resulta pertinente sintetizar las principales observaciones que emergen del análisis. Esto permitirá identificar los mayores retos y pondrá de relieve las limitaciones existentes. A modo de conclusión, esta revisión invita a la reflexión crítica sobre las posibles vías de desarrollo para avanzar hacia una Comunidad de Inteligencia europea más integrada.

En primer lugar, se ha buscado exponer de forma minuciosa las disposiciones constitucionales que limitan la capacidad de actuación europea dentro del ámbito de la seguridad. Así, dentro del ordenamiento jurídico europeo, es fundamental comprender el reparto de competencias para entender que toda cuestión relativa a la seguridad nacional es una competencia exclusiva de los Estados miembros. Sin embargo, esto no impide que la Unión Europea desarrolle iniciativas de seguridad, ya que cuenta con competencia compartida en el ELSJ y puede desarrollar la PESC por medio de cooperación intergubernamental. Esto hace que solamente actúe dentro de sus competencias otorgadas, pero que además pueda plantear políticas sobre campos que no son de su competencia directa en base a la voluntad política y las necesidades que presenta dentro de la Comunidad Internacional. Es decir, este avance depende íntegramente de la confianza entre sus miembros.

Respecto a esto último, para el desarrollo de una inteligencia europea es imprescindible tener en cuenta que la protección de datos es un derecho fundamental reconocido como parte integrante del Derecho de la Unión y desarrollado por legislación secundaria. No obstante, las diferencias en materia de protección de datos de los servicios de inteligencia nacionales se deben a la condición especial de esta competencia exclusiva. Esto merece mayor atención y supone un obstáculo para la integración.

Seguidamente, se puede ver claramente como en el proyecto europeo de integración, que inicialmente se contemplaba como eminentemente económico, ha desbordado este ámbito debido a su efecto funcionalista. Lo que se conoce hoy en día como arquitectura de seguridad es el resultado del progreso del proyecto europeo, que responde a las necesidades de seguridad dentro del marco de las relaciones internacionales. Las preocupaciones por la seguridad han sido una constante que ha marcado la integración y que

se vieron profundizadas a raíz de los atentados terroristas de principios del siglo XXI.

No obstante, la estructura actual se caracteriza por una marcada fragmentación y una falta de interoperabilidad que no solo conduce a la duplicación de esfuerzos, sino que dificulta y retrasa la toma de decisiones en la Unión Europea. La dependencia de las agencias europeas de las capacidades nacionales acentúa estas dificultades, las cuales se ven agravadas por la desconfianza entre Estados, imposibilitando la cooperación plena entre servicios y agencias.

Sumado a estos problemas, los servicios de inteligencia aúnan una tensión clásica entre el interés público y los derechos individuales, dado que implican el uso de información personal para garantizar la seguridad nacional. En este aspecto, la confianza se manifiesta como factor clave. Consecuentemente, un elemento central es el recelo que suele suscitar el funcionamiento de las instituciones internacionales, cuya naturaleza requiere métodos de trabajo diferentes a los nacionales.

Bajo estas circunstancias, el marco que regula tanto las agencias europeas como las nacionales es distinto en cada caso. A respecto a la protección de datos, aunque este sea un derecho fundamental reconocido a nivel europeo, se encuentra fragmentada y omite claramente los servicios de seguridad nacionales al encontrarse fuera de sus competencias.

Sin embargo, son los escándalos de vigilancia masiva y espionaje los que han puesto en alerta tanto a la sociedad civil como a los propios jueces y a la academia, avivando la controversia. Como resultado, el TJUE se ha pronunciado para determinar que las salvaguardas relativas a la protección de datos competen al Derecho de la Unión en cualquier ámbito. Esto se traduce en una petición para que las leyes que regulan los servicios de seguridad nacionales sean compatibles con los valores europeos y con los compromisos adquiridos por los Estados miembros.

De lo anterior se puede inferir que a día de hoy son varios los obstáculos que persisten para la integración o, si quiera, la armonización en materia de inteligencia. Entre ellos destacan la falta de voluntad para compartir información, la desconfianza, las culturas de trabajo dispares y la dificultad para adaptarse a los estándares europeos de protección de datos. Esta situación se origina en la soberanía nacional, pero el contexto internacional exige la cooperación como condición indispensable para hacer frente a las amenazas emergentes. Esta coyuntura exige replantearse las necesidades para impulsar el avance.

Pese a los diferentes marcos legales y culturas operativas, es preciso reconocer que los Estados europeos no solo comparten intereses, sino también preocupaciones. Por ello, la fundación de una Comunidad de Inteligencia europea no supone la creación de una nueva estructura, sino el replanteamiento de un marco institucional construido sobre los preexistentes valores

europeos compartidos, que cada Estado sea capaz de percibir como propio y no como ajeno.

La armonización de marcos entorno a los valores que fundamentan la identidad europea favorece la confianza mutua al ofrecer unos estándares de referencia que han sido acordados por todos los miembros de la Unión Europea. Esto incluye su amplio catálogo de derechos, uno de los hitos fundamentales del acervo comunitario. En última instancia, esto permite avanzar hacia una visión común para afrontar las amenazas globales y coordinar los recursos necesarios para responder de manera eficaz, constituyendo un paso más en el proyecto europeo.

A modo de conclusión, las posibilidades que ofrece la Comunidad de Inteligencia redundan en el fortalecimiento de la seguridad colectiva de la Unión sin menoscabar la autonomía y las competencias propias de los Estados. De esta manera, se favorece la toma de decisiones, tanto a nivel nacional como europeo, al ofrecer una plataforma capaz de procesar información de mayor alcance. Una toma de decisiones informada es esencial para la resolución de problemas y, en consecuencia, se configura como condición imprescindible para garantizar la seguridad y los derechos de la Unión Europea y sus integrantes.

## BIBLIOGRAFÍA

**Angheland, S.**, **Damen, M.**, *The future European security architecture: dilemmas for EU strategic autonomy*, European Parliamentary Research Service, 2025.

**Bureš, O.**, «Intelligence sharing and the fight against terrorism in the EU: lessons learned from Europol», en *European View*, vol. 15, 2016.

**Buzan, B.**, *People, state and fear: an agenda for international security studies in the post-Cold War era*, 2ª ed., New York, Harvester Wheatsheaf, 1991.

**Díaz-Canaleja Greciano, J. M.**, *La cooperación de inteligencia en la Unión Europea*, Instituto Español de Estudios Estratégicos, Madrid, 2014.

**Cameron, I.**, «European Union Law Restraints on Intelligence Activities», en *International Journal of Intelligence and Counterintelligence*, vol. 33, 2020.

**Celeste, E.**, **Formici, G.**, «Constitutionalizing Mass Surveillance in the EU: Civil Society Demands, Judicial Activism, and Legislative Inertia», en *German Law Journal*, vol. 25, 2024.

**Coutts, S. D.** «The Lisbon Treaty and the Area of Freedom, Security and Justice as an area of legal integration», en *Croatian Yearbook of European Law and Policy*, vol. 7, 2021.

**Craig, P.**, **De Búrca, G.**, «Competence», en *EU Law: text, cases and materials*, 7ª ed., Oxford, Oxford University Press, 2008, págs. 102-135.

**Den Boer, M.**, «Juggling the Balance between Preventive Security and Human Rights in Europe», en *Security and Human Rights*, vol. 26(2-4), 2015.

**Díaz-Canaleja Greciano, J. M.**, *La cooperación de inteligencia en la Unión Europea*, Instituto Español de Estudios Estratégicos, Madrid, 2014.

**Díaz Fernández, A. M.**, «Evolución de la cooperación europea en inteligencia», en *Varia Historia*, vol. 28(47), 2012.

**González García, A.**, «Condiciones de viabilidad para establecer un Sistema Integrado de Inteligencia Europeo», en *Grupo de Estudios en Seguridad Internacional*, vol. 9, 2018.

**González López, D.**, «La integración europea en materia de inteligencia: ¿un servicio de inteligencia europeo?», en *Studia Humanitatis Journal*, vol. 4(2), 2024

**Gutheil, M.** et al, *Study on Interoperability of Justice and Home Affairs Information Systems*, Policy Department for Citizens' Rights and Constitutional Affairs of the European Parliament, Bruselas, 2018.

**Hallinan, D.**, «A Theory of EU Data Protection Law», en *European Data Protection Law Review*, vol. 9(3), 2023.

**Kaunert, C.**, «The Area of Freedom, Security and Justice: The Construction of a 'European Public Order'», en *European Security*, vol. 14(4), 2005.

**Keohane, R.**, **Nye, J.**, *Power and Interdependence*, 4ª ed., Lognman, 1997.

**Kelemen, R. D.**, **McNamara K. R.**, «State-building and the European Union: Markets, War, and Europe's Uneven Political Development», en *Comparative Political Studies*, vol. 55(6), 2022.

**Lavenex, S.**, **Wagner, W.**, «Which European Public Order? Sources of Imbalance in the European Area of Freedom, Security and Justice», en *European Security,* vol. 16(3), 2007.

**Lonardo, L.**, «EU Law against hybrid threats: a first assessment», en *European Papers*, vol. 6(2), 2021.

**Mitsilegas, V.** et al, «Data retention and the future of large-scale surveillance: The evolution and contestation of judicial benchmarks», en *European Law Journal*, vol. 29(1-2), 2023.

**Nomikos, J. M.**, «European Union Intelligence Analysis Centre (INTCEN): Next stop to an Agency?», en *Journal of Mediterranean and Balkan Intelligence*, vol. 4(2), 2014.

**Palacios, J. M.**, «Cooperación entre servicios de inteligencia: la dimensión regional», en *Revista de Relaciones Internacionales, Estrategia y Seguridad*, vol. 16(1), 2021.

**Protopapas, G. X.**, «European Union's Intelligence Cooperation: A Failed Imagination?», en *Journal of Mediterranean and Balkan Intelligence*, vol. 4(2), 2014.

**Lyon, D.**, «Surveillance, Snowden, and Big Data: Capacities, consequences, critique», en *Big Data & Society*, vol. 1(2), 2014.

**Strmečki, S.** y **Pejaković-Đipi, S.**, «Data Protection, Privacy and Security in the context of artificial intelligence and Conventional Methods for Law Enforcement», en *EU And Comparative Law Issues and Challenges Series*, vol. 7, 2023.

**Tilly, C.**, *Coerción, capital y los Estados europeos: 990-1990*, Basil Blackwell, Cambridge, 1990.

# LA IMPORTANCIA DE LA COMUNICACIÓN EN LA INTELIGENCIA ESTRATÉGICA

**Inmaculada Crespo González**
**Patricia Pérez Rodríguez**
*Analistas de Inteligencia en Grupo FCC*

## 1. Introducción

Actualmente, los procesos de toma de decisiones estratégicas en las grandes empresas enfrentan constantemente un entorno volátil, incierto, complejo y ambiguo. Además, el fenómeno de la digitalización global y la rápida transformación geopolítica ha hecho que las organizaciones, tanto de naturaleza pública como privada, reconozcan la necesidad de implementar y desarrollar estructuras cognitivas que sean capaces de anticipar escenarios, detectar amenazas emergentes y ofrecer respuestas ante múltiples desafíos simultáneos, a través de una interpretación de los datos. En este marco, la inteligencia estratégica se ha afianzado como un elemento esencial para el entendimiento del entorno, la administración del riesgo y la elaboración de objetivos fundamentales a largo plazo. Su finalidad no es solo impedir imprevistos, sino reducir los riesgos inherentes de cada contexto y convertir el conocimiento fragmentado en ventajas estratégicas.

La inteligencia estratégica como disciplina, proceso y resultado surge oficialmente después de la Segunda Guerra Mundial, cuando los países comenzaron a desarrollar sus propias estructuras sofisticadas de inteligencia y el conocimiento pasó a ser un instrumento de poder para anticiparse ante el adversario y no una mera acumulación de datos. Desde ese momento, su desarrollo ha sido caracterizado por el uso de técnicas analíticas precisas adoptando un enfoque sistémico de los eventos para poder ampliar su alcance más allá del fenómeno bélico y militar, abarcando sectores como la economía, la tecnología, la energía o la diplomacia, mostrando su naturaleza transversal y multidimensional.

Es importante mencionar que el objetivo principal de la inteligencia estratégica es una suma de numerosos factores que no pretenden proporcionar

certezas absolutas, sino reducir la incertidumbre de un contexto en constante evolución para mejorar los procesos de toma de decisiones. Las fases y etapas que se desarrollan en este proceso implican la recolección y análisis de los datos, la interpretación contextualizada del conflicto y el desarrollo de un producto de inteligencia que sea aplicable a cada situación. Sin embargo, un análisis exhaustivo no es adecuado si no se logra transmitir su contenido de forma efectiva, y es por ello por lo que la dimensión comunicativa cobra una gran relevancia, donde el saber debe ser entendido para ser aplicado. La comunicación en inteligencia, especialmente la inteligencia, se ha convertido en una parte indispensable que relaciona al analista con el encargado de tomar decisiones. Una inteligencia estratégica debe ser correctamente comunicada para que resulte útil en términos operativos.

Además, la inteligencia narrativa sugiere utilizar los fundamentos del *storytelling* para organizar y comunicar el conocimiento analítico. Esta técnica ha despertado un interés creciente en los estudios estratégicos por su habilidad para captar atención, provocar emoción y facilitar la memorización. En un contexto donde los tomadores de decisiones lidian con una carga de información continua, la narrativa ayuda a organizar la información, simplificar el entendimiento de situaciones complejas y promover la acción. De este modo, la narración es capaz de proporcionar claridad, inmediatez, y adaptabilidad estratégica.

Por otro lado, existen diferentes modelos de comunicación narrativa que se pueden utilizar según la situación o la audiencia a la que se dirigen. La pirámide invertida facilita la priorización de la información esencial desde el comienzo, lo cual es especialmente valioso en situaciones con tiempo escaso. La narración persuasiva construye un hilo argumental desde la exposición del problema a resolver hasta la solución sugerida. Finalmente, los escenarios hipotéticos muestran interpretaciones diferentes del futuro, facilitando la visualización de riesgos y oportunidades antes de que se concreten.

Así mismo, la transformación de las amenazas actuales ha llevado a que los conflictos no se resuelvan únicamente en el ámbito físico, sino que muchas confrontaciones se desarrollan ahora en el terreno de los datos, las percepciones, las narrativas y la guerra cognitiva, la información engañosa constante, los asaltos a infraestructuras clave, o los ciberconflictos. En la actualidad, la habilidad para transmitir de manera efectiva los resultados analíticos se convierte en algo tan relevante como el propio análisis.

Igualmente, la inteligencia estratégica contemporánea demanda un enfoque adaptable y versátil. El contexto global se distingue por la irrupción de agentes no estatales, debilidades tecnológicas, fenómenos transnacionales, transformaciones sistémicas profundas, competencia por recursos naturales, polarización política y cambios poblaciones. Todos estos factores son algunos de los elementos principales que configuran esta nueva estructura de riesgos.

Este documento tiene como objetivo principal examinar la relación entre la inteligencia estratégica y la comunicación efectiva. A lo largo de los cuatro apartados desarrollados a continuación, se tratará la evolución, los fundamentos y características principales de la inteligencia estratégica, para posteriormente poder entrar en la fase de difusión del ciclo de inteligencia, en la que se examinará el rol del *storytelling* en la creación de productos analíticos. A continuación, se evaluará la capacitación requerida del analista frente a estas nuevas exigencias, y finalmente se presentarán conclusiones y reflexiones a futuro.

En conclusión, entender la inteligencia estratégica sin considerar su aspecto comunicativo sería tan insuficiente como creer que la narrativa puede reemplazar la carencia de rigor analítico. Únicamente la combinación armónica entre estos dos componentes, análisis exhaustivo y comunicación efectiva posibilita la creación de inteligencia realmente valiosa para la toma de decisiones.

## 2. Definición y fundamentos de la inteligencia estratégica

La inteligencia estratégica ha progresado de forma notable desde sus inicios en contextos bélicos hacia una dimensión empresarial aplicable a diversas áreas del poder. Después de la Segunda Guerra Mundial, la inteligencia empezó a convertirse en una función institucionalizada dentro de las estructuras gubernamentales de cada nación, especialmente en países como Estados Unidos y en el marco de la Unión Europea, extendiendo así su marco de actuación desde el espionaje táctico para adelantarse a movimientos del enemigo, hasta la planificación estratégica y detallada a largo plazo. Esta transformación ha estado caracterizada por la urgencia de hacer elecciones más conscientes frente a contextos geopolíticos en constante cambio y cada vez más complejos e interconectados. La inteligencia estratégica se ha constituido en una herramienta fundamental para captar las dinámicas del contexto internacional y no únicamente un recurso subordinado a la política exterior[1].

La definición actual de inteligencia estratégica se entiende como una disciplina que convierte datos fragmentados en conocimiento elaborado que es capaz de guiar y apoyar decisiones estratégicas en contextos de alta incertidumbre. El principal objetivo es ayudar a los líderes de cada ámbito en la comprensión de factores geopolíticos y en la previsión de acontecimientos futuros en situaciones de gran inestabilidad. Esta materia se basa en actividades organizadas como la recopilación, el análisis, la integración de

1. Ransom, H., «Strategic Intelligence and Foreign Policy», *World Politics* 27 (1), 1974, págs. 131-146.

información y la generación de conocimiento con utilidad. Por lo tanto, no se trata únicamente de reunir información, sino de crear percepciones que sean capaces de disminuir la duda y respaldar decisiones intencionadas y oportunas[2].

Una de las cualidades más relevantes de la inteligencia estratégica es su organización en diferentes niveles, siendo estos: estratégico, operativo y táctico. Esta organización posibilita una conexión coherente entre la perspectiva a largo plazo, la coordinación intermedia y la implementación directa. El nivel estratégico es el que ofrece el marco teórico y la dirección general del camino, el nivel operativo se encarga de convertir esta visión en planes específicos, y el nivel táctico realiza acciones tangibles e inmediatas en el campo. Esta complementariedad entre los tres niveles garantiza que las decisiones que se toman sean coherentes desde la primera fase de planificación hasta la última de ejecución, permitiendo una integración de manera efectiva en las diferentes partes del proceso de decisión[3].

A sí mismo, la función de la inteligencia estratégica en la actualidad ha adquirido notable importancia debido a la aparición de amenazas complejas que no se ajustan a las categorías convencionales de conflicto. Actores no gubernamentales, ataques cibernéticos, conflictos híbridos, *fake news* y sabotajes a infraestructuras esenciales son algunos de los peligros que enfrentan actualmente los estados y entidades. Estos retos requieren una inteligencia que no solo observe, sino que entienda con precisión las interrelaciones globales y las dinámicas desiguales que definen al siglo XXI. En realidad, el contexto político actual suele politizar la inteligencia, lo que puede alterar el análisis a menos que se fijen estándares éticos definidos y una separación efectiva entre el productor y el usuario de inteligencia[4].

El proceso de toma de decisiones basado en la inteligencia estratégica se transforma en un recurso esencial a través de un proceso que incluye varias fases como la identificación del problema, la evaluación del contexto, la formulación de sugerencias y la puesta en práctica de decisiones. Estas etapas están relacionadas y demandan tanto un pensamiento organizado como una flexibilidad en la interpretación. La eficacia del proceso está influenciada por factores como el capital humano, la utilización correcta de tecnologías, y la combinación de enfoques DAFO (Debilidades, Amenazas, Fortalezas, Oportunidades) con una perspectiva futura[5].

---

2. Véase Heidenrich, J. G., «The State of Strategic Intelligence» *Studies in Intelligence* 51 (2), 2007.

3. Paiuc, D., A. Săniută, A. M. Teacu Părincu, «Strategic Intelligence: A Semantic Leadership Perspective», *Encyclopedia* 4, 2024, págs. 785-798.

4. Eisenfeld, B., «The Intelligence Dilemma: Proximity and Politicization. Analysis of External Influences», *Journal of Strategic Security* 10 (2), 2017, págs. 77-96.

5. Santos Nauca Torres, E., Chávarry Ysla, P. del R., «La inteligencia estratégica para la toma de decisiones gerenciales», *Revista Tzhoecoen* 12 (1), 2020, págs. 10-18.

Además, el estudio estratégico en inteligencia no puede separarse del crecimiento profesional del analista. La normalización analítica en la comunidad de inteligencia, impulsada por esfuerzos como las Directivas del director de Inteligencia Nacional en EE. UU. ha sido esencial para asegurar estándares compartidos de objetividad, pertinencia y exactitud en los informes generados. En este aspecto, la profesionalidad del analista y la rigurosidad metodológica son fundamentos de la confiabilidad del producto de inteligencia, y la importancia de la inteligencia estratégica no está solo en su habilidad de observación, sino en su capacidad para crear proyecciones futuras. Las habilidades de previsión, creación de visión y colaboración son fundamentales para prever cambios, desarrollar estrategias y establecer consensos en las organizaciones. Estas competencias forman la base de la inteligencia estratégica en el liderazgo y son aplicables tanto en el sector público como en el privado[6].

Históricamente, la inteligencia ha funcionado como un recurso para anticipar sorpresas estratégicas, pero su finalidad no debe restringirse a la prevención de crisis, sino que debe guiar una comprensión profunda del entorno y facilitar una respuesta adaptativa y oportuna, incluso sin certezas absolutas. El principal objetivo radica en manejar la incertidumbre en lugar de tratar de eliminarla totalmente, ya que es un factor inherente a los contextos complejos pero cuya utilidad la hacen una herramienta esencial para líderes que desean operar con información, anticipación y flexibilidad.

La inteligencia estratégica debe considerarse como un proceso mental organizado que transforma información dispersa en saber práctico para la acción, y que requiere una secuencia analítica en la que se manejan grandes volúmenes de datos (frecuentemente inciertos, contradictorios o parciales) mediante técnicas de evaluación, inferencia y síntesis que faciliten una comprensión integral y anticipatoria de un fenómeno. Además, este procedimiento debe seguir normas analíticas estrictas que garanticen objetividad, pertinencia, exactitud y oportunidad en los productos de inteligencia, especialmente en contextos donde los errores pueden tener consecuencias estratégicamente devastadoras[7].

En este contexto, la inteligencia estratégica es simultáneamente un producto, un proceso y una organización. Como producto, simboliza el resultado definitivo de un ciclo de tratamiento, capaz de ser utilizado por tomadores de decisiones políticas, militares o empresariales. Este proceso consiste en etapas lógicas: planificación, recolección, validación, análisis, difusión y retroalimentación. Finalmente, a nivel empresarial, conlleva la presencia de estructuras estables, personal especializado con pensa-

6. Reinhold, D., Russo, C. M., Eisenfeld, B., «Analytical Standards in the Intelligence Community» *Journal of Strategic Security* 14 (1), 2020, págs. 106-121.

7. Britten, S., «Intelligence Failures Are Analytical Failures», Counter Terrorist Trends and Analyses 10 (7), 2018, págs. 12-18.

miento crítico y sistemas tecnológicos de soporte que garanticen la continuidad de la labor de inteligencia. En la actualidad ya no es suficiente con reunir información a través de tecnologías avanzadas, sino que los analistas deben ser capaces de reconocer patrones, identificar elementos esenciales y anticipar resultados. Los fallos más significativos se originan por deficiencias en el análisis, no en la recolección de datos. Así, la calidad del análisis es un elemento crucial en la efectividad de la inteligencia estratégica. Esto implica promover una cultura organizativa centrada en la claridad metodológica, la evaluación entre colegas, el registro de conclusiones y el aprendizaje constante. Asimismo, para que la inteligencia sea efectiva en la estrategia, el analista debe formar parte del equipo estratégico, en lugar de comportarse como un participante externo que proporciona productos finales sin entender las verdaderas necesidades de los tomadores de decisiones. Solo de esta manera la información puede transformarse en conocimiento útil.

Por otro lado, el diagnóstico es fundamental, ya que representa el momento en que se identifica el conflicto o la amenaza. Es necesario interpretar señales tenues, reconocer actores clave, comprender las dinámicas estructurales y las interdependencias. Esta etapa debe prevenir tanto el alarmismo exagerado como la confianza desmedida, y fundamentarse en una lógica de alerta temprana y sensata. La elaboración de estrategias, que es la segunda fase del proceso, necesita convertir la inteligencia analítica en decisiones específicas de acción. Aquí surge la necesidad de conectar la inteligencia con la política y la gestión estratégica, y esta conexión demanda no solo un análisis de situaciones, sino también la inclusión de componentes de inteligencia emocional, cultural y organizacional, que faciliten entender la receptividad y factibilidad de las decisiones sugeridas. Finalmente, durante la fase de implementación, la inteligencia actúa como un apoyo técnico y táctico para facilitar la coordinación entre partes involucradas y valorar riesgos operativos, dando lugar a la fase de monitoreo y control donde la inteligencia estratégica se vuelve a incorporar nuevamente como herramienta de retroalimentación[8].

En la actualidad, en un entorno multipolar, inestable y colmado de información, la inteligencia estratégica se encuentra ante desafíos en aumento, en el que los líderes actuales no pueden depender de lógicas lineales o respuestas estándar; deben actuar en contextos donde los problemas son *«maliciosos»* (*wicked problems*), careciendo de soluciones obvias, con varias dimensiones e intereses contradictorios. En este escenario, la inteligencia estratégica proporciona un esquema para manejar la complejidad, prever efectos y organizar decisiones en situaciones de incertidumbre.

8. Véase Fernández Villacañas Marín, M. A., «Strategic Intelligence Management and Decision Process: An Integrated Approach in an Exponential Digital Change Environment», Cap. 4, 2020.

# 3. Fase de difusión en el ciclo de inteligencia: cómo aplicar la inteligencia narrativa

La difusión es la fase en la que un producto analítico deja de ser un conjunto de hallazgos y se convierte en decisión posible. No es un trámite final, sino un proceso comunicativo donde se negocian significado, riesgo y acción. Su objetivo no es «entregar datos», sino hacerlos utilizables por audiencias específicas, políticas, estratégicas u operativas, en ventanas de tiempo concretas. Por ello, claridad, oportunidad, formato y adecuación al destinatario son determinantes de calidad tanto como la solidez de las fuentes o de los métodos analíticos empleados[9].

## 3.1. ¿Qué es la inteligencia narrativa?

Llamamos inteligencia narrativa al uso deliberado de estructuras narrativas (personajes/actores, causalidades, tramas y marcos temporales) para organizar, interpretar y comunicar información estratégica en contextos de incertidumbre. A diferencia del «cuento» o mero *storytelling* persuasivo, la inteligencia narrativa somete las historias a criterios de plausibilidad, coherencia explicativa y contraste con la evidencia; ayuda a distinguir entre lo verosímil y lo verdadero, a explorar hipótesis alternativas y a alinear inferencias con pruebas[10]. En su vertiente aplicada, el campo recoge técnicas para escuchar y mapear narrativas (quién las impulsa, cómo se propagan, qué resonancias culturales activan) y para anticipar su impacto en percepciones públicas y comportamientos de actores relevantes[11].

## 3.2. Por qué la comunicación efectiva es decisiva en inteligencia

La calidad analítica es condición necesaria pero no suficiente: sin una comunicación analítica clara, concisa y adaptada a la audiencia, la mejor estimación pierde valor. La tradición profesional, de Sherman Kent a los manuales contemporáneos de estilo, insiste en que escribir con precisión, concreción y libre de jerga no es cosmética, sino parte del oficio: lo que no puede explicarse con claridad difícilmente está bien pensado[12]. Desde la psicología cognitiva

9. Véase Verreault, E., «Understanding the Intelligence Cycle», AKTEK, 2023.

10. Véase Van Gelder, T., «Storytelling in Intelligence: Theoretical Foundations» *International Journal of Intelligence and Counterintelligence*, 2025.

11. Véase Brito, M. «Narrative Intelligence: Using Storytelling and Technology to Reshape Perception», BRITOPIAN, 2023.

12. Véase Davis, J., *Sherman Kent and the Profession of Intelligence Analysis*. Washington, DC: CIA, 2020.

del análisis, además, se sabe que los sesgos y la excesiva confianza ponen en riesgo tanto el conocimiento como su transmisión. Este riesgo se puede mitigar a través de la inversión en estructuras argumentativas transparentes y en la aplicación de técnicas que analicen distintas hipótesis para mejorar la recepción por parte del decisor[13]. En términos operativos, difundir bien implica:

a) seleccionar el formato adecuado (informe extenso, *brief*, *dashboard*, *readout* oral);

b) ajustar el nivel técnico al receptor;

c) explicitar incertidumbres (con escalas probabilísticas y lenguaje calibrado);

d) entregar a tiempo y de forma segura[14].

## 3.3. Storytelling y valor explicativo en informes estratégicos

El *storytelling* analítico sirve para reducir fricción cognitiva: segmenta la información, jerarquiza causalidades, conecta señales débiles con tendencias y genera modelos mentales compartidos entre analistas y decisores. Una buena narrativa estratégica no oculta la incertidumbre; la enmarca (por ejemplo, con advertencias sobre supuestos críticos y vacíos informativos). Las guías de redacción en la comunidad de inteligencia recomiendan estructurar informes con mensajes clave, evidencias trazables, juicios calibrados y advertencias bien destacadas; todo ello articulado de forma concisa y libre de jerga[15]. Asimismo, la visualización, líneas de tiempo, diagramas de actores, mapas de influencia, no reemplaza la narrativa: la apoya, haciendo visibles relaciones causales y supuestos. La norma es *«menos es más»:* gráficos simples, leyendas claras y un hilo conductor que señale qué cambia, para quién y por qué ahora.[16]

## 3.4. Ejemplo CHALLENGER: cuando la narrativa falla

El 28 de enero de 1986, el transbordador *Challenger* se desintegró a los 73 segundos del despegue. La Comisión Rogers identificó la falla de las juntas tóricas (*O-rings*) del *booster* como causa inmediata. Sin embargo, señaló

13. Véase Heuer, R. J., *Psychology of Intelligence Analysis*. Washington, DC: Central Intelligence Agency, 1999.

14. Véase Verreault, E., «Understanding the Intelligence Cycle», AKTEK, 2023.

15. Véase CENTRAL INTELLIGENCE AGENCY, *Style Manual & Writers Guide for Intelligence Publications*. Washington, DC: CIA, 2012.

16. Véase DEFENSE INTELLIGENCE AGENCY, *Style Manual for Intelligence Production*. Washington, DC: CIA, 2017.

también fallas organizativas y de comunicación: información crucial sobre cómo afectaban las bajas temperaturas y objeciones de ingenieros no fueron recibidas eficazmente por los decisores en las horas críticas previas al lanzamiento[17]. Esta narrativa interna («volamos con riesgo controlado») venció a la narrativa técnica («el riesgo es inaceptable con frío»), produciendo un marco explicativo que desalineó hechos, inferencias y decisiones[18]. Incluso décadas después, revisiones históricas subrayan el papel de la cultura que embellecen las advertencias: cuando los procesos de difusión no recalcan adecuadamente la relevancia de escenarios de fallo, el decisor recibe una historia más limpia, pero menos verdadera[19].

### 3.5. Subrayado final: comunicar bien es parte de «pensar bien»

La inteligencia narrativa potencia la difusión cuando: (1) expone supuestos, vacíos y alternativas; (2) calibra lenguaje probabilístico y niveles de confianza; (3) adapta el relato a la audiencia; y (4) protege el disenso analítico y la señalización de riesgo. En suma, comunicar bien no es decorar: es epistemología aplicada al servicio de la decisión[20].

## 4. Modelos de narrativas estructuradas en inteligencia

La implementación de narrativas estructuradas en inteligencia estratégica responde a una necesidad fundamental: transformar información densa o dispersa en relatos coherentes que faciliten la comprensión rápida, el recuerdo efectivo y una acción decisiva. Cuando la narrativa sigue una forma deliberada, como la pirámide invertida o escenarios hipotéticos, cumple funciones cognitivas esenciales: simplificar, enfocar y motivar la toma de decisiones. Las narrativas estructuradas ayudan a segmentar la experiencia en unidades manejables, lo que contribuye a que los tomadores de decisiones procesen la información sin sentirse abrumados. En particular, la estructura narrativa ayuda a *«dar sentido»,* distinguiendo lo relevante de lo accesorio[21]. Además, las historias bien tejidas se integran más fácilmente en los esque-

17. Véase NASA, *Report of the Presidential Commission on the Space Shuttle Challenger Accident*. Washington, DC, 1986.

18. Véase Maher, R., «History as Cause: Columbia and Challenger», NASA, 2006.

19. Véase WASHINGTON POST, «*William R. Lucas, NASA Director during Challenger Disaster, Dies at 101*», Washington Post, 2025.

20. Véase CENTRAL INTELLIGENCE AGENCY, *Style Manual & Writers Guide for Intelligence Publications*. Washington, DC: CIA, 2012.

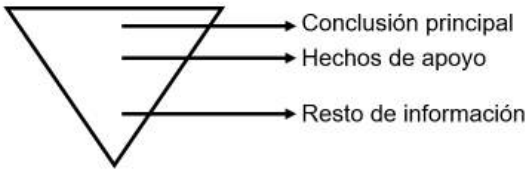
21. Véase Edmunds, D., Morris, J. A., *Can Stories Shape Strategy? Narrative-Structured Information and Strategic Decision Making.* Academy of management proceedings, 2000.

mas mentales existentes y se recuerdan con mayor facilidad, gracias a sus múltiples puntos de conexión y su capacidad emocional para impactar en la memoria. Esto aumenta la probabilidad de que las ideas clave sean consideradas y recordadas por los decisores.

## 4.1. Pirámide invertida

Este modelo, bien conocido en el periodismo, prioriza la información más importante desde el inicio y luego refina con detalles secundarios[22]. En el contexto de inteligencia estratégica, esto se traduce en presentar primero el mensaje fundamental o la conclusión central, seguido por los argumentos y datos de soporte. Así se garantiza que audiencias con tiempo limitado reciban lo más relevante de inmediato.

Ilustración I. Estructura narrativa de pirámide invertida.




Fuente: Elaboración propia.

## 4.2. Narrativa persuasiva

La narrativa persuasiva sigue una estructura clásica: inicio (planteamiento del problema o contexto) —desarrollo (presentación de evidencia y argumentos)— resolución (recomendaciones o curso de acción). Este modelo promueve una progresión lógica que guía al lector hacia una comprensión integral y una conclusión justificada. En inteligencia, emplear esta estructura asegura que el receptor comprenda primero el contexto, luego evalúe la evidencia y finalmente asimile las recomendaciones estratégicas como una consecuencia natural.

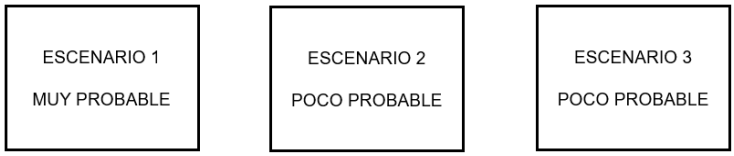
## 4.3. Escenarios hipotéticos

El uso de escenarios es una técnica analítica consolidada. Permite explorar futuros posibles —tanto favorables como desfavorables— para preparar a

22. Pöttker, H., «News and Its Communicative Quality», *Journalism Studies* 4 (4), 2003, págs. 501-511. Taylor & Francis.

la organización frente a eventos imaginables[23]. Al construir estos escenarios, los analistas pueden desafiar supuestos y estimular la reflexión sobre distintas alternativas, fortaleciendo la capacidad de anticipación y adaptación.

Ilustración II. Ejemplo de diversificación
de escenarios hipotéticos por probabilidad.




Fuente: Elaboración propia.

### 4.4. Narrativas colaborativas y micro-narrativas

Un aspecto particularmente relevante es el uso de micro-narrativas colaborativas en plataformas de inteligencia colectiva. En investigaciones recientes, se ha observado cómo analistas construyen «microhistorias» fragmentarias durante la deliberación —por ejemplo, vía chats o interacciones en línea— que luego se integran en una narrativa mayor, ideal y compartida[24]. Estas micro-piezas permiten avanzar en la hipótesis, explorar alternativas y reenfocar el análisis. En contextos ágiles, esta práctica favorece la creación de relatos conjuntos que representan mejor la diversidad de percepciones y evidencias, enriqueciendo la difusión final[25].

## 5. Formación del analista para la redacción de informes estratégicos

La elaboración de informes estratégicos constituye una de las competencias centrales del analista de inteligencia. La calidad del documento no depende únicamente de los datos disponibles, sino de la capacidad del analista para procesarlos, interpretarlos y presentarlos de manera que apoyen la toma de decisiones. En este sentido, la formación del analista no se limita al dominio técnico de fuentes y metodologías, sino que incorpora dimensio-

23. Véase Saletta, M., Kruger, A., Primoratz, T., Barnett, A., Gelder, T., Horn, R., *The Role of Narrative in Collaborative Reasoning and Intelligence Analysis*. Journals plos org, 2020.

24. Véase Norambuena, B., Mitra, T., North, C., *Narrative Sensemaking: Strategies for Narrative Maps Construction*. IEEE Visualization Conference, 2021.

25. Véase MIN, S, y Park, J., *Mapping Out Narrative Structures and Dynamics Using Networks and Textual Information.* Cornell University: Computation and Language, 2016.

nes cognitivas, comunicativas y adaptativas que determinan la utilidad final del producto de inteligencia[26]. Además, las nuevas herramientas de procesamiento de información, como aquellas con inteligencia artificial, introducen oportunidades y desafíos adicionales que modifican la forma de redactar los informes[27].

## 5.1. Dimensiones de formación para el analista

La preparación del analista estratégico debe contemplar, en primer lugar, el desarrollo del pensamiento crítico y de habilidades analíticas. No basta con recopilar datos; es preciso interpretarlos dentro de un marco conceptual que permita distinguir entre información relevante y ruido, identificar sesgos, y evaluar la fiabilidad de las fuentes. Los errores cognitivos y las trampas analíticas son una de las principales amenazas para la objetividad del análisis, y solo el entrenamiento y el uso de técnicas estructuradas puede mitigarlos[28]. En segundo lugar, la comunicación es un componente esencial. Un informe estratégico no solo transmite hallazgos, sino que busca persuadir y orientar a los tomadores de decisiones en situaciones críticas o con gran incertidumbre. La claridad expositiva, el uso adecuado de narrativas y la organización coherente del texto son tan importantes como la solidez del análisis. En tercer lugar, la adaptabilidad estratégica se ha convertido en una competencia crítica en entornos caracterizados por la aceleración tecnológica y la creciente complejidad de los escenarios. Los analistas deben ser capaces de integrar enfoques prospectivos en el proceso de inteligencia, lo que exige flexibilidad metodológica[29].

## 5.2. Avance de las herramientas para la redacción de informes

La evolución tecnológica ha impactado de manera directa en la práctica de la inteligencia. Si en décadas anteriores la redacción de informes se apoyaba en bases de datos rudimentarias y en la experiencia personal del analista, hoy el abanico de herramientas disponibles es mucho más amplio

26. Véase Marrin, S., *Improving Intelligence Analysis: Bridging the Gap between Scholarship and Practice*. New York: Routledge, 2012.

27. Véase NATIONAL RESEARCH COUNCIL, *Intelligence Analysis for Tomorrow: Advances from the Behavioral and Social Sciences*. Washington, DC: The National Academies Press. Cap. 6: «Communication», 2011.

28. Véase Heuer, R. J., Pherson., R. H., *Structured Analytic Techniques for Intelligence Analysis*. 2.ª ed. Washington, DC: CQ Press, 2015.

29. Véase Werro, A., Nitzl, C., Borghoff, U. M., «On the Role of Intelligence and Business Wargaming in Developing Foresight», 2024.

y sofisticado[30]. Uno de los avances más significativos ha sido el desarrollo del procesamiento de lenguaje natural (en adelante PLN), que permite analizar grandes volúmenes de texto, identificar patrones y generar resúmenes automáticos. Estas capacidades facilitan la detección de tendencias en tiempo real, la disminución de redundancias y la estructuración de narrativas básicas. Existen ya plataformas que, a partir de datos numéricos y textuales, producen borradores que pueden servir de base para realizar informes estratégicos.

En el plano operativo, se observa un creciente interés por la automatización de informes. Herramientas de *Natural Language Generation* (NLG) convierten datos estructurados en informes, por ejemplo, indicadores económicos, registros de seguridad o métricas de riesgo. De esta forma, el analista puede concentrar sus esfuerzos en la interpretación de los resultados y en la formulación de recomendaciones estratégicas, en lugar de invertir tiempo en tareas meramente descriptivas[31].

En cuanto a los productos de inteligencia, la tecnología abre posibilidades de diversificación. Actualmente, se pueden encontrar visualizaciones interactivas, *dashboards* dinámicos y simulaciones prospectivas que facilitan la comprensión de escenarios complejos. Sin embargo, la incorporación de narrativas sigue siendo esencial: la forma en que se estructuran los hallazgos influye directamente en la manera en que los líderes perciben dichas amenazas y oportunidades[32].

## 5.3. Ejemplo práctico: construcción de un informe narrativo

Para ilustrar estas dinámicas, resulta útil presentar un caso hipotético de redacción de un informe estratégico en el marco de una crisis energética con implicaciones geopolíticas. Imaginemos un escenario en el que un país europeo altamente dependiente del gas enfrenta interrupciones súbitas en el suministro debido a tensiones diplomáticas con su principal proveedor. La situación genera volatilidad en los mercados, presión social interna y alteración de los aliados regionales. En la fase inicial, el analista recopila información de fuentes abiertas: declaraciones oficiales, reportes

30. Véase Berger, L., Borghoff, U. M., Conrad, G., y Pickl, S., «Intelligence Education Made in Europe», *arXiv*, 2024.

31. Véase NATIONAL ACADEMIES OF SCIENCES, ENGINEERING, AND MEDICINE, «A Decadal Survey of the Social and Behavioral Sciences: A Research Agenda for Advancing Intelligence Analysis», Washington, DC: The National Academies Press. Cap. 4: «The Work of the Intelligence Analyst», 2019.

32. Véase Marrin, S., *Improving Intelligence Analysis: Bridging the Gap between Scholarship and Practice*. New York: Routledge, 2012.

del sector energético, movimientos en los mercados internacionales y estimaciones de organismos multilaterales. Con el apoyo de herramientas de PLN, se identifican patrones en las narrativas mediáticas y en los discursos políticos, lo que permite anticipar posibles líneas de acción de los actores involucrados. El informe narrativo resultante podría estructurarse en tres secciones principales:

a) Descripción de la situación actual: interrupciones en el flujo de gas, impacto en los precios domésticos y medidas inmediatas adoptadas por el gobierno.

b) Escenarios prospectivos:

   i. normalización parcial del suministro en el corto plazo mediante acuerdos diplomáticos;

   ii. prolongación de la crisis con búsqueda de proveedores alternativos;

   iii. escalada hacia un conflicto regional con repercusiones en la seguridad energética de toda la Unión Europea.

c) Recomendaciones estratégicas: diversificación urgente de fuentes de energía, establecimiento de mecanismos de cooperación con socios regionales, inversión en renovables para reducir la dependencia y fortalecimiento de las reservas estratégicas nacionales.

En este proceso, una herramienta de generación automática podría aportar resúmenes diarios sobre la evolución del mercado y los discursos de los actores, mientras que el analista aporta coherencia, selecciona los escenarios más plausibles y formula recomendaciones. La combinación de ambas dimensiones (automatización y juicio crítico humano) resulta decisiva para construir un producto de inteligencia de alto valor añadido.

## 5.4. Consideraciones finales

La formación del analista en la redacción de informes estratégicos debe entenderse como una síntesis entre capacidades cognitivas, habilidades comunicativas y manejo de herramientas tecnológicas. El pensamiento crítico y la claridad expositiva siguen siendo irremplazables, pero se ven potenciados por sistemas de procesamiento automático que facilitan la gestión de grandes volúmenes de información. El desafío no consiste únicamente en dominar nuevas herramientas, sino en mantener la capacidad de juicio y la responsabilidad ética que distinguen al analista humano de la máquina. En última instancia, los informes estratégicos no son simples documentos descriptivos: son narrativas que orientan decisiones de alto impacto en contextos de incertidumbre. Por ello, la verdadera formación del analista debe preparar al profesional para integrar datos, narrativas y tecnología en un mismo producto, siempre al servicio de la toma de decisiones informadas.

# 6. Conclusión

La inteligencia estratégica se presenta hoy como una disciplina en constante evolución, cuyo valor radica tanto en la rigurosidad de sus métodos analíticos como en la capacidad de comunicar con eficacia los resultados obtenidos. A lo largo de este artículo se ha puesto de relieve que la inteligencia no puede concebirse únicamente como un proceso de recopilación y procesamiento de datos, sino como una práctica integral que transforma información dispersa en conocimiento aplicable y, sobre todo, útil para la toma de decisiones en escenarios complejos e inciertos. La clave de su efectividad reside en que el producto analítico logre reducir la incertidumbre de los contextos actuales, ofreciendo a los líderes un mapa interpretativo que facilite la acción estratégica.

En este marco, la dimensión comunicativa se ha revelado como un factor determinante. El análisis más sofisticado carece de valor si no es transmitido con claridad, pertinencia y oportunidad a quienes deben actuar sobre su base. La inteligencia estratégica no se limita a producir diagnósticos; necesita convertirlos en relatos comprensibles y persuasivos, capaces de guiar a decisores que operan bajo presión, con horizontes de tiempo limitados y frente a un flujo incesante de información. De ahí que la narrativa, en sus diversas formas —pirámide invertida, estructuras persuasivas o escenarios prospectivos—, se constituya como una herramienta esencial para dotar de coherencia y fuerza explicativa al análisis, al tiempo que permite visibilizar riesgos, alternativas y posibles cursos de acción.

Los ejemplos históricos y contemporáneos demuestran que una falla en la comunicación puede resultar tan grave como un error en la recolección o en la interpretación de los datos. La tragedia del *Challenger*, analizada como un caso de narrativa fallida, subraya que cuando la comunicación suaviza advertencias críticas o elimina matices relevantes, los decisores reciben una versión distorsionada de la realidad que compromete sus elecciones. Esta lección sigue vigente: comunicar bien no es un complemento estético, sino una condición intrínseca de la práctica de la inteligencia. Pensar bien exige también explicar bien, con transparencia en los supuestos, claridad en las inferencias y honestidad en la exposición de incertidumbres.

El contexto actual, marcado por la digitalización, la proliferación de actores no estatales, los conflictos híbridos, la desinformación y la guerra cognitiva, plantea exigencias aún mayores. En este escenario, los analistas deben contar con competencias que trasciendan la dimensión técnica. No basta con dominar fuentes y metodologías; resulta imprescindible desarrollar pensamiento crítico, conciencia ética y habilidades comunicativas que permitan construir productos de inteligencia capaces de influir en la acción. Del mismo modo, la irrupción de herramientas tecnológicas basadas en inteligencia artificial ofrece oportunidades inéditas para procesar grandes volúmenes de datos y generar insumos analíticos, pero refuerza a la vez la nece-

sidad de preservar el juicio humano como garante de pertinencia, contexto y responsabilidad.

Por todo ello, la formación del analista en el siglo XXI debe concebirse como un proceso integral en el que confluyen tres dimensiones: la analítica, orientada al rigor metodológico y a la objetividad de los resultados; la comunicativa, centrada en la transmisión eficaz y adaptada del conocimiento; y la tecnológica, enfocada en la integración de nuevas herramientas sin renunciar al criterio crítico. La inteligencia estratégica será valiosa en la medida en que logre articular estos tres componentes, evitando tanto el tecnicismo vacío como la narrativa carente de fundamento.

En síntesis, este trabajo permite afirmar que la inteligencia estratégica contemporánea solo alcanza su máximo potencial cuando análisis y comunicación actúan de manera armónica. Una sin la otra resulta insuficiente: el rigor analítico sin narrativa conduce a productos incomprensibles o inoperantes; la narrativa sin rigor analítico deriva en relatos seductores pero vacíos de valor. La conjunción equilibrada de ambas dimensiones no solo optimiza la calidad de los informes estratégicos, sino que garantiza su impacto en la toma de decisiones, convirtiendo la inteligencia en un instrumento real de poder, anticipación y adaptación.

Finalmente, los desafíos del futuro demandan que la inteligencia estratégica continúe renovándose para responder a contextos de creciente incertidumbre. Esto implica fomentar culturas organizativas basadas en la transparencia, la colaboración interdisciplinar y el aprendizaje constante; reforzar la ética profesional frente a la tentación de manipular o sesgar el conocimiento; y asumir que la comunicación, lejos de ser un paso final, constituye un proceso transversal que acompaña todo el ciclo de inteligencia. Solo de esta manera será posible construir una inteligencia estratégica que no se limite a describir el mundo, sino que contribuya de manera efectiva a transformarlo, ofreciendo a los líderes herramientas sólidas para decidir en entornos cada vez más inciertos y desafiantes.

## BIBLIOGRAFÍA

**Berger, L., Borghoff, U. M., Conrad, G., Pickl, S.**, «Intelligence Education Made in Europe», *arXiv*, 2024.

**Brito, M.**, «Narrative Intelligence: Using Storytelling and Technology to Reshape Perception», BRITOPIAN, 2023.

**Britten, S.**, «Intelligence Failures Are Analytical Failures», Counter Terrorist Trends and Analyses 10 (7), 2018, International Centre for Political Violence and Terrorism Research.

**CENTRAL INTELLIGENCE AGENCY**, *Style Manual & Writers Guide for Intelligence Publications*. Washington, DC: CIA, 2012.

**CENTRAL INTELLIGENCE AGENCY**, *Style Manual & Writers Guide for Intelligence Publications*. Washington, DC: CIA, 2012.

**Davis, J.**, *Sherman Kent and the Profession of Intelligence Analysis*. Washington, DC: CIA, 2020.

**DEFENSE INTELLIGENCE AGENCY**, *Style Manual for Intelligence Production*. Washington, DC: CIA, 2017.

**Edmunds, D.** y **Morris, J. A.**, *Can Stories Shape Strategy? Narrative-Structured Information and Strategic Decision Making.* Academy of management proceedings, 2000.

**Eisenfeld, B.**, «The Intelligence Dilemma: Proximity and Politicization — Analysis of External Influences», *Journal of Strategic Security* 10 (2), 2017, University of South Florida Board of Trustees.

**Fernández, M. A.**, «Strategic Intelligence Management and Decision Process: An Integrated Approach in an Exponential Digital Change Environment», Cap. 4, 2020.

**Heidenrich, J. G.**, «The State of Strategic Intelligence», *Studies in Intelligence* 51 (2), 2007.

**Heuer, R. J.**, *Psychology of Intelligence Analysis*. Washington, DC: Central Intelligence Agency, 1999.

**Heuer, R. J.**, y **Pherson, R. H.**, *Structured Analytic Techniques for Intelligence Analysis*. 2.ª ed. Washington, DC: CQ Press, 2015.

**Maher, R.**, «History as Cause: Columbia and Challenger», NASA, 2006.

**Marrin, S.**, *Improving Intelligence Analysis: Bridging the Gap between Scholarship and Practice*. New York: Routledge, 2012.

**Marrin, S.**, *Improving Intelligence Analysis: Bridging the Gap between Scholarship and Practice*. New York: Routledge, 2012.

**Min, S.** y **Park, J.**, *Mapping Out Narrative Structures and Dynamics Using Networks and Textual Information.* Cornell University: Computation and Language, 2016.

**NASA**, *Report of the Presidential Commission on the Space Shuttle Challenger Accident*. Washington, DC, 1986.

**NATIONAL ACADEMIES OF SCIENCES, ENGINEERING, AND MEDICINE**, «A Decadal Survey of the Social and Behavioral Sciences: A Research Agenda for Advancing Intelligence Analysis» Washington, DC: The National Academies Press, Cap. 4: «The Work of the Intelligence Analyst», 2019.

**NATIONAL RESEARCH COUNCIL**, *Intelligence Analysis for Tomorrow: Advances from the Behavioral and Social Sciences*. Washington, DC: The National Academies Press. Cap. 6: «Communication», 2011.

**Norambuena, B.**, **Mitra, T.**, **North, C.** *Narrative Sensemaking: Strategies for Narrative Maps Construction*. IEEE Visualization Conference, 2021.

**Paiuc, D.**, **Săniută, A.**, **Teacu Părincu, A. M.**, «Strategic Intelligence: A Semantic Leadership Perspective», *Encyclopedia* 4, 2024.

**Pöttker, H.**, «News and Its Communicative Quality.» *Journalism Studies* 4 (4), 2003, Taylor & Francis.

**Ransom, H.**, «Strategic Intelligence and Foreign Policy» *World Politics* 27 (1), 1974, Johns Hopkins University Press.

**Reinhold, D., Russo, C. M., Eisenfeld, B.**, «Analytical Standards in the Intelligence Community», *Journal of Strategic Security* 14 (1), 2020, University of South Florida Board of Trustees.

**Saletta, M., Kruger, A., Primoratz, T., Barnett, A., Gelder, T., Horn, R.**, *The Role of Narrative in Collaborative Reasoning and Intelligence Analysis*. Journals plos org, 2020.

**Santos Nauca Torres, E., Chávarry Ysla**, **P. del R.**, «La inteligencia estratégica para la toma de decisiones gerenciales», *Revista Tzhoecoen* 12 (1), 2020.

**Van Gelder, T.**, «Storytelling in Intelligence: Theoretical Foundations», *International Journal of Intelligence and Counterintelligence*, 2025.

**Verreault, E.**, «Understanding the Intelligence Cycle», AKTEK, 2023.

**WASHINGTON POST**, «*William R. Lucas, NASA Director during Challenger Disaster, Dies at 101*», Washington Post, 2025.

**Werro, A., Nitzl, C., Borghoff**, **U. M.** , «On the Role of Intelligence and Business Wargaming in Developing Foresight», 2024.

# LA COMUNICACIÓN ESTRATÉGICA Y EL LENGUAJE SOBRE DEFENSA, SEGURIDAD E INTELIGENCIA: ANÁLISIS DE CASOS EN ESPAÑA

**Raquel Pinilla Gómez**

*Profesora Doctora en Universidad Rey Juan Carlos*

## 1. Introducción

Vivimos en un mundo globalizado y convulso en el que, en las últimas décadas, asistimos con inquietud a la extensión de conflictos armados e incremento de la violencia, las amenazas terroristas y los riesgos globales. Escenarios bélicos de guerra e invasión que veíamos lejanos a nuestras fronteras se han ido aproximando y han penetrado en el corazón mismo de sociedades que antaño se sentían seguras y defendidas. Una buena muestra de ello la constituyen los ataques del 11 de septiembre de 2001 sobre las Torres Gemelas de Nueva York, el atentado del 11 de marzo de 2004 en trenes de Cercanías de Madrid o el llevado a cabo contra la sede del semanario Charlie Hebdo, en París, el 7 de enero de 2015, entre otros muchos. Más recientemente, hemos visto nacer y extenderse conflictos bélicos como el originado tras la invasión rusa de Ucrania, iniciada el 24 de febrero de 2022, que continúa hasta nuestros días; o el de Israel y Palestina, que comenzó con la ofensiva israelí el 7 de octubre de 2023 tras el ataque del grupo terrorista Hamás y que no solo se mantiene hoy, sino que ha escalado a otros países de su entorno geopolítico.

Por todo ello, resulta imprescindible que la ciudadanía acceda y conozca la información sobre las acciones que nuestros Estados realizan en política de defensa, seguridad e inteligencia. Además, los Estados necesitan afianzar su presencia en el discurso público y comunicar de manera eficaz su actividad. Como ciudadanos de esta realidad compleja y cambiante marcada por tantos conflictos y amenazas, debemos conocer de primera mano qué instituciones velan por nuestra seguridad, cómo funcionan y en base a qué criterios toman sus decisiones. En este sentido, en España, la comunicación estratégica de las Fuerzas Armadas, del Ministerio de Defensa o del Centro Nacional de Inteligencia resulta básica en la transmisión de esa información a la sociedad. Sin embargo, ¿estamos familiarizados los ciudadanos españoles

con la cultura de defensa e inteligencia?, ¿nos preocupamos por mantenernos informados en estas materias? En los últimos años, han surgido plataformas digitales como «Seguridad y Defensa» (SegDef) con ese espíritu divulgativo, pero riguroso, para ofrecer análisis de estos temas tanto a los medios de comunicación como a la ciudadanía, porque «por una serie de condicionamientos históricos y sociales, la nación española parece estar menos ducha e informada en estas materias que los países de su entorno»[1]. Las redes sociales, los medios digitales y los formatos de *podcasting*, entre otros, han contribuido también a «democratizar» y popularizar esa cultura de la defensa y la inteligencia. El artículo 2 de la *Ley Orgánica 5/2005, de 17 de noviembre, de la Defensa Nacional* establecía la finalidad de la política de defensa:

> «La política de defensa tiene por finalidad la protección del conjunto de la sociedad española, de su Constitución, de los valores superiores, principios e instituciones que en ésta se consagran, del Estado social y democrático de derecho, del pleno ejercicio de los derechos y libertades, y de la garantía, independencia e integridad territorial de España. Asimismo, tiene por objetivo contribuir a la preservación de la paz y seguridad internacionales, en el marco de los compromisos contraídos por el Reino de España».

La protección de la sociedad española, de la Constitución y de los valores democráticos constituye, por tanto, un objetivo esencial para la seguridad, y la defensa es uno de los medios principales para alcanzarla. Pero ¿son conscientes los ciudadanos españoles de la relevancia de esta misión?, ¿conocen las instituciones que toman las decisiones en materia de defensa para preservar la paz y la seguridad?, ¿entienden la realidad material que subyace a términos como *defensa*, *seguridad*, *inteligencia* o *amenaza híbrida*? En este trabajo, partimos de esas preguntas de investigación con los siguientes tres objetivos principales:

a) definir los conceptos clave de este campo semántico de la defensa, la seguridad y la inteligencia;

b) presentar el concepto de *comunicación estratégica* y ofrecer una síntesis de los principales retos que plantea dicha comunicación en estos ámbitos, especialmente en el ámbito de la desinformación;

c) analizar casos de comunicación estratégica y del uso del lenguaje que realizan tres portales web esenciales para la información ciudadana en estas materias: el Centro Superior de Estudios de la Defensa Nacional (CESEDEN), el Departamento de Seguridad Nacional (DSN) y el Centro Nacional de Inteligencia (CNI).

1. *segdef.com* es una plataforma digital «que reúne a académicos, periodistas, estudiosos y expertos de varios campos para ofrecer información y análisis en los medios y ambientes académicos» de ámbitos como la seguridad interior, la defensa, la ciberseguridad, el terrorismo, la geoestrategia, las relaciones internacionales, la inteligencia, etc. Así mismo, está presente en Facebook, X, Instagram y Telegram.

## 2. Conceptos clave en el ámbito de la defensa, la seguridad y la inteligencia

Como en cualquier disciplina académica, la conceptualización y la acotación terminológica son imprescindibles para identificar, clasificar y analizar las materias objeto de estudio de manera científica. Todos los conceptos clave sufren una evolución a lo largo del tiempo, condicionada por los diferentes contextos históricos y sociales. Así como las tácticas y estrategias militares han evolucionado con el paso de los años y los avances tecnológicos, los conceptos y la interpretación que se hace de ellos también lo han hecho. Un término como *guerra*, por ejemplo, no reproduce una misma realidad si pensamos en épocas históricas como la Edad Media o la II Guerra Mundial que si nos aproximamos a los conflictos bélicos contemporáneos, con nuevas dimensiones comunicativas y digitales en su materialización y conceptualización como las que corresponden a la *guerra híbrida*[2]. Además, desde un punto de vista lingüístico, las campañas militares o los conflictos bélicos son una fuente inagotable de acuñación de nuevos términos «que conforman lo que se conoce como el vocabulario de la guerra»[3]. Así sucede en el caso de la invasión rusa de Ucrania, que ha extendido a través de los medios de comunicación lexemas como *operación militar especial* (eufemismo usado por Rusia para evitar el término *invasión*), *Occidente colectivo* (bloque occidental liderado por Estados Unidos y la Unión Europea), *neonazismo* (acusación de Vladímir Putin contra Volodímir Zelenski y el Gobierno de Ucrania), *Anti-Rusia* (según Rusia, un proyecto de Estados Unidos para que Ucrania se convierta en todo lo opuesto a Rusia), *multipolar* (el orden mundial pretendido por Rusia), etc.

En este apartado se han seleccionado los conceptos básicos que un ciudadano debería conocer: *defensa*, *seguridad* e *inteligencia*. Así mismo, en el ámbito comunicativo se presentan y analizan *cultura de seguridad* y *cultura de inteligencia*. Se cierra con una breve aproximación a lo que constituyen las *Fuerzas Armadas*, al apreciar un cierto desconocimiento entre la ciudadanía de cuál es el contenido exacto al que alude este término.

---

2. El concepto de *guerra híbrida* (o *estrategia híbrida*) no es nuevo, pero sí se ha extendido en los medios a raíz de la guerra iniciada tras la invasión rusa de Ucrania. Hace referencia a los conflictos bélicos actuales que se libran «en nuevos 'campos de batalla', en nuevos escenarios de la comunicación (lo que hoy se conoce también como el ecosistema comunicativo y mediático): ciberataques, campañas de desinformación, propaganda, censura, uso interesado y manipulador de las redes sociales, etc.»; Pinilla-Gómez, R., «Análisis del discurso, poder y guerra de informaciones: el lenguaje y la comunicación en la invasión rusa de Ucrania», en *El discurso como herramienta de control social*, 2023, Peter Lang.

3. AGENCIA EFE (24/08/2022), El vocabulario de la guerra. Disponible en: https://www.fundeu.es/noticia/el-vocabulario-de-la-guerra/

## 2.1. Defensa, seguridad e inteligencia

*Defensa*. En el *Diccionario de la Lengua Española* -DLE- (Real Academia Española -RAE-) no se recoge una acepción específica del concepto de *defensa* para el contexto que estamos tratando, sino una de carácter general en su tercera acepción: «amparo, protección, socorro», que nos ofrece el contenido semántico básico del término. En la *Directiva de Defensa Nacional 2020* sí encontramos una definición del término *defensa* en el ámbito que nos ocupa: «la Defensa es un servicio público que contribuye a mantener la seguridad y los derechos y libertades de los españoles en cualquier situación». En este documento, el más importante en materia de defensa tras la *Ley Orgánica de Defensa Nacional 5/2005, de 17 de noviembre, de la Defensa Nacional* se hace una mención específica a cómo ha evolucionado este concepto, desde «ser un concepto orientado a gestionar amenazas concretas a contribuir, con su propia idiosincrasia, a un sistema de Seguridad Nacional integrador». La defensa, por tanto, está al servicio de la protección ciudadana.

*Seguridad*. El DLE introduce el término *seguridad* en la locución adjetiva *de seguridad* «dicho de un cuerpo o fuerza de las Administraciones públicas: que vela por la seguridad de los ciudadanos. *Agente de seguridad*». Por la seguridad de un país, efectivamente, velan las instituciones y organizaciones de la defensa, que reciben información de los servicios de inteligencia. En la siguiente cita de la *Directiva de Defensa Nacional 2020* queda reflejada la relación entre la defensa y la seguridad: «Ya no existen problemas exclusivos de la Defensa, pero la Defensa forma parte de la solución a cualquier problema de Seguridad». En nuestra sociedad actual, los problemas de seguridad nacional son muchos, incluyendo los desafíos no convencionales que provienen de los entornos cibernéticos: amenazas informáticas, campañas de desinformación, *hackeos* masivos, etc. Así pues, la seguridad de una nación no es una tarea baladí. En resumen:

> «el concepto de seguridad válido para el siglo XXI debe ser amplio y dinámico, dirigido a cubrir todos los ámbitos concernientes a la seguridad del Estado y de sus ciudadanos, que son variables según las rápidas evoluciones del entorno estratégico y abarcan desde la defensa del territorio a la estabilidad económica y financiera, o la protección de las infraestructuras críticas, pasando por el cambio climático, el riesgo frente a pandemias o los clásicos desafíos de la delincuencia»[4].

*Inteligencia*. El DLE incluye *inteligencia* en el sintagma *servicio de inteligencia* en su octava acepción: «Organización del Estado que proporciona al poder ejecutivo análisis e información para mejorar la toma de decisiones estratégicas orientadas a prevenir o neutralizar amenazas y a defender los

4. https://www.uv.es/instituto-criminologia-ciencias-penales/es/investigacion/lineas-investigacion/inteligencia-seguridad.html

intereses nacionales». Los servicios de inteligencia españoles, dependientes del Ministerio de Defensa, radican en el Centro Nacional de Inteligencia,

> «el organismo público responsable de facilitar al presidente del Gobierno y al Gobierno de la nación las informaciones, análisis, estudios o propuestas que permitan prevenir y evitar cualquier peligro, amenaza o agresión contra la independencia o la integridad territorial de España, los intereses nacionales y la estabilidad del Estado de derecho y sus instituciones»[5].

## 2.2. Cultura de defensa y cultura de inteligencia

En la dimensión comunicativa de este ámbito de la defensa, la seguridad y la inteligencia, resulta fundamental el conocimiento y puesta en valor que la sociedad tenga sobre sobre ellas. El ciudadano tiene el derecho de estar informado sobre los diferentes mecanismos y agentes de protección, y el Estado tiene el deber de transmitirle el valor de la seguridad. En este sentido, surgen los conceptos de *cultura de defensa* y *cultura de inteligencia*, relacionados con todas las acciones e iniciativas de alfabetización sobre estos temas por parte de los organismos nacionales como el Gobierno de la nación o el Ministerio de Defensa. El fin último es proporcionar a la ciudadanía el conocimiento suficiente para entender cómo trabaja el Estado en pro de su seguridad antes los desafíos y las amenazas nacionales e internacionales.

*Cultura de defensa.* Hemos visto ya que la política de defensa de España «determina los objetivos de la defensa nacional y los recursos y acciones necesarias para obtenerlos»[6]. Las instituciones y organizaciones encargadas de dichas políticas tienen diferentes herramientas y leyes para poder desarrollar esas acciones, partiendo de la *Constitución española* de 1978 y la *Carta de las Naciones Unidas* de 1945. En el contexto de esa política de defensa se enmarcan la *Ley Orgánica de Defensa Nacional 5/2005*, la *Estrategia de Seguridad Nacional 2021* o la *Directiva de Defensa Nacional*. La cultura de defensa es necesaria para hacer llegar al ciudadano que España tiene medios y capacidad para defenderse y responder ante las posibles amenazas y que este es un fin primordial de las autoridades de su país.

> «La necesidad de promover el desarrollo de la cultura de defensa se nombra en el artículo 31 de la ***Ley Orgánica de Defensa Nacional 5/2005***, que establece como finalidad ''que la sociedad española conozca, valore y se identifique con su historia y con el esfuerzo solidario y efectivo mediante el que las Fuerzas Armadas salvaguardan los intereses nacionales''»[7].

5. https://www.cni.es/sobre-el-cni/objetivos-y-valores

6. https://www.defensa.gob.es/defensa/politicadefensa/

7. Santiago Marín, J. M. et al., *Documento de Opinión IEEE 75/2024. Pedagogía de la cultura de la defensa*, Instituto Español de Estudios Estratégicos, 2024, pág. 7.

Deberíamos plantearnos si en España existe una cultura de defensa suficiente y cómo se despierta el interés de la ciudadanía por ella. Además de las iniciativas del Gobierno o de las Fuerzas Armadas, como campañas publicitarias, los medios de comunicación contribuyen en mayor o menor medida a esta cultura de defensa, especialmente a raíz de la proliferación de conflictos bélicos en los últimos años y la consecuente aparición de analistas y periodistas especializados en cuestiones de seguridad y defensa. Las series de ficción o *docuseries* de las televisiones y de las plataformas digitales han servido también para dar a conocer y popularizar la labor de las Fuerzas Armadas en organismos y escenarios internacionales de seguridad y defensa[8].

*Cultura de inteligencia.* El objetivo fundamental de una cultura de inteligencia es que la ciudadanía esté informada y participe como conocedora de este campo específico de la seguridad y la defensa: la inteligencia[9]. Además, es importante también que los conceptos relacionados con los servicios y las estrategias de inteligencia de un país formen parte de una estrategia más amplia de abordaje de estos temas en el ámbito académico y en el de comunicación social -medios de comunicación-, así como de relaciones con los contextos económicos, empresariales, culturales, políticos, etc[10].

El concepto de *cultura de inteligencia* se puede definir como:

> «conjunto de conocimientos que la sociedad debe tener sobre la necesidad, el fin y la función de un servicio de inteligencia, de manera que perciba como propias las cuestiones relacionadas con su seguridad, su libertad y la defensa de sus intereses»[11].

## 2.3. Fuerzas Armadas

El último concepto analizado es el de *Fuerzas Armadas*. Si bien puede parecer que su significado es obvio para el ciudadano, resulta fundamental para las culturas de defensa e inteligencia que este entienda bien a qué hace referencia exactamente. El artículo 10 del Capítulo II de la *Ley Orgánica 5/2005, de 17 de noviembre, de la Defensa Nacional* hace explícita la

8. Algunos programas y series recientes son, por ejemplo, *FAS* (2016), que enseña el día a día de los militares españoles; *La Unidad* (2020), que muestra el trabajo de una unidad policial secreta que lucha contra el terrorismo yihadista; o *Fuerza de paz* (2021) ambientada en una misión de paz en Guinea Ecuatorial.

9. https://www.defensa.gob.es/Galerias/documentacion/ficheros/SGT-bibliografia-Inteligencia.pdf

10. Véase Sansó-Rubert, D., Pulido-Gragera, J., «Cultura de inteligencia y sociedad», en *URVIO. Revista Latinoamericana De Estudios De Seguridad*, 34, 2022.

11. Esteban Navarro, M. A., *Glosario de Inteligencia*, Madrid: Servicio de Publicaciones del Ministerio de Defensa de España, 2007, págs. 68-69.

organización de las Fuerzas Armadas, a las que define en el punto 1 con las siguientes palabras:

> «Las Fuerzas Armadas son el elemento esencial de la defensa y constituyen una entidad única que se concibe como un conjunto integrador de las formas de acción específicas de cada uno de sus componentes: el Ejército de Tierra, la Armada y el Ejército del Aire».

Por tanto, el sintagma *Fuerzas Armadas* constituye un nombre colectivo en el que se integran los conocidos coloquialmente como *los tres ejércitos*: el Ejército de Tierra, la Armada y el Ejército del Aire y del Espacio, bajo la dirección operativa del Estado Mayor de la Defensa.

## 3. Retos de la comunicación estratégica sobre defensa, seguridad e inteligencia

En un sentido amplio, prácticamente todos los procesos humanos de comunicación resultan estratégicos puesto que la persuasión y la argumentación se encuentran en la base intencional de las interacciones comunicativas: convencer al otro. En origen, *estrategia* es un término que procede del léxico militar, pero extendido en el ámbito general de la comunicación. Los hablantes desarrollamos y utilizamos constantemente estrategias de comunicación para ser más eficientes desde un punto de vista comunicativo y para solventar los problemas que van surgiendo en las destrezas de expresión, comprensión e interacción; por ejemplo, cuando no entendemos una palabra y pedimos ayuda a nuestro interlocutor o cuando no recordamos o no sabemos una palabra y usamos una paráfrasis para describirla.

En el contexto específico de defensa, seguridad e inteligencia, el concepto de *comunicación estratégica* está más restringido en cuanto a su referencia. La comunicación estratégica forma parte de las políticas desarrolladas por los poderes públicos nacionales, entendidas en sentido genérico como «los programas sectoriales y las acciones concretas que emanan de las instituciones de gobierno como resultado de la interacción política»[12]. La comunicación estratégica siempre presenta tres características: es producto de una autoridad pública, supone una acción deliberada y tiene objetivos previamente establecidos[13]. Aunque, en principio, la comunicación estratégica tiene su origen en las instituciones públicas, en la actualidad hay otros muchos agentes comunicativos que también la implementan, como las organizaciones no gubernamentales o los medios de comunicación.

12. Molina, I., *Conceptos fundamentales de Ciencia Política*, Alianza Editorial, Madrid, 1998, pág. 98.

13. Sánchez Benítez, S., *Documento de Opinión IEEE 21/2011. La comunicación estratégica como política pública*, Instituto Español de Estudios Estratégicos, 2011, pág. 3.

Sergio Sánchez Benítez ofrece la siguiente definición operativa de *comunicación estratégica*:

> «Política pública aprobada e implementada por una autoridad gubernamental y dirigida a potenciar las ventajas competitivas y a consolidar la posición de una Nación, mediante el intercambio (emisión/recepción) proactivo y constante de mensajes con audiencias seleccionadas y a través de diversos medios y canales»[14].

Un hito importante en el ámbito español, que pone de relieve la necesidad de la comunicación estratégica de la defensa, es el documento que lleva por título *Directiva de la Ministra de Defensa sobre Comunicación Estratégica*, publicado en noviembre de 2017, en el que encontramos la siguiente definición de comunicación estratégica de la defensa:

> «la integración de todas las funciones y capacidades de comunicación —civiles y militares— con otras actividades con la finalidad de comprender y determinar el entorno de la información, e informar, influir o persuadir en las audiencias identificadas para lograr los objetivos nacionales de Defensa».

El objetivo de este documento es «proporcionar las directrices para desarrollar la comunicación estratégica en todos los ámbitos y niveles del Ministerio de Defensa -estratégico, operacional y táctico- bajo la dirección de la Ministra».

Un aspecto fundamental de la comunicación estratégica de la defensa y su impacto en la percepción por parte de la ciudadanía reside en la importancia de la transparencia en la comunicación de defensa ya que dicha transparencia en las acciones y decisiones de defensa puede generar y aumentar la confianza y el apoyo entre los ciudadanos. De acuerdo con este objetivo, «la política de comunicación del Ministerio de Defensa promueve que la sociedad conozca a sus Fuerzas Armadas y, de esta manera, se identifique con ellas»[15].

Casos significativos de comunicación estratégica en el ámbito público e institucional son los que se producen, por ejemplo, en situaciones de crisis y emergencias, la llamada comunicación de riesgo, como en los desastres naturales, las pandemias o los atentados terroristas. En estas coyunturas, los ciudadanos necesitan una información clara y precisa de las autoridades, con un lenguaje inequívoco, sin ambigüedades, directo y comprensible; así lo pudimos comprobar durante la pandemia de Covid-19, en la que no solo eran importantes los mensajes oficiales de salud pública, sino también, la presencia pública y mediática de las Fuerzas Armadas o de las Fuerzas y Cuerpos de

14. Ibid., pág. 7.

15. Moréu Munáiz, F., «Evolución de la cultura de defensa en la última década», en *Arbor, Ciencia, Pensamiento y Cultura* 190 (765), 2014, pág. 1.

Seguridad del Estado como transmisores de esos mensajes gubernamentales y como garantía del control y la estabilidad nacionales. Resultan esclarecedoras en este sentido las recomendaciones sobre el lenguaje dadas por la Organización Panamericana de la Salud (2009):

> «No utilice más de tres ideas al mismo tiempo. Use una gramática simple, de oraciones cortas y en voz activa. No abuse de las cifras o los números. Evite las jergas técnicas y las siglas. Si usa términos poco conocidos, acompañe su mensaje de un glosario. Utilice el lenguaje según la audiencia que ha definido. Evite mensajes que refuercen estereotipos culturales o étnicos».

Desde el ámbito de la lingüística aplicada, también se aborda el análisis de la comunicación estratégica de riesgo y se proponen modelos lingüísticos para analizar las estrategias discursivas léxicas, sintácticas, etc., así como la posición enunciativa de los emisores de los mensajes (disposición ante los receptores, transparencia, etc.), lo cual nos permite entender mejor el interés que despierta el estudio de la comunicación estratégica, de cara a conseguir cada vez más eficacia así como minimizar los errores y las dificultades comunicativas de los potenciales receptores.

Como hemos visto hasta ahora, el papel y las campañas de comunicación por parte de las instituciones públicas en torno a la defensa y la seguridad resultan fundamentales para que la ciudadanía no considere estos asuntos ajenos a ella. Las relaciones entre la comunicación y la política son complejas y sin duda «la comunicación desempeña un papel cada vez más destacado en la política interna de los Estados»[16].

Uno de los retos principales es que los medios de comunicación establezcan adecuadamente un puente informativo entre las instituciones y la ciudadanía para difundir de manera regular los mensajes que promuevan la cultura de defensa e inteligencia. Los medios de comunicación pueden influir en la percepción pública sobre la defensa y la seguridad ya que seleccionan los temas en función de la llamada *agenda setting* y establecen, por tanto, los focos de cobertura sobre los que la sociedad va a informarse, con la consiguiente generación de la opinión pública.

Otro reto importante es el que tiene que ver con la educación y la sensibilización sobre la defensa en el sistema educativo. Enseñar a los niños y jóvenes en el marco de los currículos de enseñanza qué instituciones velan por la seguridad, cómo se organizan y cuáles son sus misiones es fundamental para conseguir una ciudadanía bien informada y educada en temas de defensa, y supone una estrategia efectiva en la lucha contra las campañas de desinformación y bulos. Sobre el fenómeno de la desinformación profundizamos a continuación, en vista de su relevancia actual.

16. Sánchez Benítez, S., *Documento de Opinión IEEE 21/2011. La comunicación estratégica como política pública*, Instituto Español de Estudios Estratégicos, 2011, pág. 1.

## 3.1. El fenómeno de la desinformación

Uno de los problemas globalizados del mundo actual es la desinformación, un fenómeno multidimensional en el punto de mira de la crisis reputacional de las democracias y de las instituciones tradicionales. En todas sus dimensiones comunicativas, las campañas de desinformación se han convertido en una seria amenaza para la credibilidad institucional y los valores democráticos. Asistimos en el ecosistema público al auge de bulos e informaciones maliciosas que intoxican los discursos públicos y generan confusión entre los ciudadanos. Se consideran como hitos de origen de la desinformación y la posverdad la campaña electoral de Donald Trump en el año 2016 o la comunicación mediática y social en torno a la pandemia de Covid-19. La desinformación afecta también al ámbito de las noticias relacionadas con la cultura de la defensa, en aspectos tan importantes para la opinión pública como la visión que pueda tener la ciudadanía de las Fuerzas Armadas, los cuerpos y fuerzas de seguridad del Estado, los poderes del Estado (legislativo, ejecutivo y judicial) o las instituciones públicas más relevantes.

En el ámbito de las noticias relacionadas con la defensa en España, por ejemplo, se registran casos de bulos en torno a la vuelta del servicio militar obligatorio, cuya prestación, anunciada el 9 de marzo de ese mismo año por el entonces ministro de defensa Federico Trillo, fue suspendida el 31 de diciembre de 2001. El portal de verificación de noticias Maldita.es[17] publicaba el 25 de abril de 2025[18] el artículo «Bulos y desinformaciones sobre la vuelta del servicio militar obligatorio y los españoles yendo a la guerra», en el que desmentía diferentes bulos sobre dicha vuelta del servicio militar, con vídeos y audios manipulados, o sobre el compromiso del presidente del gobierno Pedro Sánchez de que los españoles sean los primeros ciudadanos europeos en ir a «Ucrania a pegar tiros».

De la importancia que tiene el impacto de la desinformación en torno a la seguridad nacional da buena cuenta una de las áreas de actuación del Departamento de Seguridad Nacional, con la creación específica de un Foro contra las campañas de desinformación que desarrolla sus trabajos y publica sus resultados en la página web del DSN[19]. Su vocación didáctica hacia la ciudadanía se ve claramente en el capítulo 1 de esta publicación, en el que se

17. Maldita.es es un portal web dedicado a registrar y desmentir bulos, «las mal llamada fake news», en un ecosistema mediático y social en el que son armas de desinformación y en el que «los desinformadores son cada vez más» (maldita.es). Sus herramientas periodísticas de trabajo son: Maldito Bulo, Maldita Hemeroteca, Maldita Ciencia, Maldito Dato, Maldita Te Explica y Maldita Tecnología.

18. https://maldita.es/malditobulo/20250425/bulos-desinformaciones-servicio-militar-guerra-jovenes/

19. https://www.dsn.gob.es/index.php/es/publicaciones/otras-publicaciones/trabajos-foro-contra-campanas-desinformacion-iniciativas-2024

recogen 125 términos del ámbito de las campañas de desinformación, con la voluntad de evitar ambigüedades y confusiones en su uso, explicando las connotaciones y diferencias entre términos como *fake news*, *desinformación*, *bulo*, *malinformation*, etc.

Otro ejemplo de estudio de desinformación, en este caso en torno a los poderes del Estado, lo encontramos en el contexto de la huelga convocada en España, en el mes de julio de 2025, por todas las asociaciones de jueces y fiscales (a excepción de las llamadas *progresistas*), contra dos iniciativas legislativas promovidas por el gobierno de Pedro Sánchez en relación con la carrera judicial. Los representantes de estas asociaciones denunciaban los bulos que se han extendido, mayoritariamente por redes sociales, con el propósito de pervertir sus reivindicaciones y ofrecer a la opinión pública una imagen tergiversada y maliciosa de sus peticiones. Los convocantes manifestaban que los agentes creadores de los bulos -medios que identificaban afines con el Gobierno o incluso desde el propio Gobierno- no desmentían sus motivos para convocar la huelga, sino que habían entrado «a la «guerra sucia» de desmontar sus reivindicaciones con acusaciones sesgadas, cuando no directamente falsas, como por ejemplo, acusar a los jueces que siguieron la huelga de estar «en contra de las becas» o «de la entrada en la carrera de los hijos de obreros» o de que «no verán descontada la parte correspondiente en sus salarios y que, en realidad, han disfrutado de unas vacaciones pagadas»[20].

## 4. La comunicación y el lenguaje de las instituciones de defensa, seguridad e inteligencia: CESEDEN, DSN y CNI

La comunicación hacia el ciudadano por parte de las instituciones españolas en el ámbito de la defensa, la seguridad y la inteligencia se realiza básicamente mediante canales digitales. A través de ellos el ciudadano puede informarse y conocer la visión y las acciones que se llevan a cabo, estableciendo así una relación muy valiosa para una sociedad democrática como la nuestra. En este apartado analizamos las estrategias de comunicación y el lenguaje de tres de esos canales digitales: el del CESEDEN, el del DSN y el del CNI. Sabedores del poder del lenguaje como elemento transmisor, pero también en muchas ocasiones perfilador e incluso constructor de la realidad, las propias instituciones buscan adecuar su lenguaje y su tono a los canales comunicativos y a los potenciales receptores de los mensajes. El léxico y el discurso militares resultan una fuente de estudio para lingüistas y estudiosos

20. El Confidencial, 05/07/2025, «Guerra sucia» contra los jueces durante su huelga: «Tratan de convertirnos en villanos», https://www.elconfidencial.com/espana/2025-07-05/guerra-sucia-contra-los-jueces-durante-su-huelga-tratan-de-convertirnos-en-villanos_4165768/

del discurso *polemológico*. Aspectos que despiertan interés son, entre otros, «el recurso al eufemismo y, en cierto modo, a la utilización de palabras, en mayor o menor medida, asépticas», ya que en el contexto militar es habitual recurrir a términos eufemísticos para evitar palabras tabú relacionadas con la guerra, la violencia, etc. Dos ejemplos que recoge Germán Moya Hernández son: en el ámbito bélico se habla de *bajas* o *caídos* en lugar de *muertos* y en las noticias sobre la Guerra del Golfo, se utilizaba la expresión *salidas* de la fuerza aérea norteamericana en lugar de *ataques*[21].

Las categorías que vamos a analizar en las tres páginas web seleccionadas como casos de estudio son las siguientes:

a) Organización y jerarquización de la macroestructura informativa.

b) Registro lingüístico y tono institucional, es decir, las variaciones diastrática y diafásica utilizadas: lenguaje más o menos técnico o formal y uso de acrónimos, capacidad explicativa de dichos términos.

c) Estrategias discursivas empleadas para generar confianza y credibilidad, construcción de la imagen de autoridad y búsqueda de legitimación.

## 4.1. El Centro Superior de Estudios de la Defensa Nacional (CESEDEN)

El CESEDEN, organismo del Ministerio de Defensa, con sede en Madrid,

> «es el centro docente militar conjunto al que corresponde impartir la enseñanza de los Altos Estudios de la Defensa y contribuir (...) a la confluencia de los diferentes sectores sociales en la tarea común que tenemos todos los ciudadanos de defender España».

Su labor es el estudio y la investigación de la paz, la seguridad, la defensa y la política militar, a través de la impartición de cursos y enseñanzas de perfeccionamiento, pero también, como se indica en su web, «satisfacer la curiosidad de los que no conocen nuestras actividades». Por tanto, hay una clara vocación alfabetizadora en torno a la cultura de la defensa, dirigida en primer lugar a los profesionales de las Fuerzas Armadas y de las administraciones públicas, pero también a la sociedad en su conjunto, lo cual resulta fundamental para generar conocimiento público de esta institución y su labor entre los ciudadanos. Los Altos Estudios de la Defensa «permitirán difundir, entre determinados sectores de la sociedad, la cultura de seguridad y defensa, para lograr una unidad de esfuerzo en la consecución de los objetivos nacionales de seguridad y defensa nacional»[22].

---

21. Véase Moya Hernández, G., «El lenguaje militar. Tabú, eufemismo y disfemismo», en *Revista Tonos digital* 1, 2001.

22. https://www.defensa.gob.es/ceseden/ense%C3%B1anza/altos-estudios-de-la-defensa

En relación con la organización macroestructural y la jerarquización de la información que aparece en el portal, se observa una estructura modular y secuenciada, con las siguientes secciones: Conócenos, Enseñanza Militar, Publicaciones, Cultura de Defensa, Diplomacia de Defensa, Historia Militar (recensiones sobre libros de temática militar, referencias de las actividades realizadas -no actualizado desde 2022- y enlaces de páginas de otros organismos e instituciones relacionadas) y Actividades. En esta web se prioriza la navegación temática y cronológica, y se permite descargar directamente muchos de los documentos referenciados, lo cual supone una facilidad de acceso para cualquier usurario interesado.

En cuanto al registro lingüístico y el tono, se utiliza un tono académico y un registro formal, propio de una institución educativa militar, pero con vocación docente. El lenguaje es técnico, con abundancia de términos especializados en defensa y estrategia, aunque accesibles en su significado ya que dichos términos aparecen explicados: *fuerza conjunta* (unidad operativa compuesta por diferentes ramas de las Fuerzas Armadas), *defensa colectiva* (OTAN/UE), *estrategia de cooperación internacional en defensa* (en el marco de alianzas como la OTAN y la UE), *operaciones internacionales de paz y estabilidad* (misiones militares en el extranjero con fines humanitarios o de seguridad). Los acrónimos siempre están desarrollados cuando aparecen por primera vez, por ejemplo *Instituto Español de Estudios Estratégicos* (IEEE), *Departamento de Cultura y Diplomacia de Defensa* (DCDD) o *Escuela Superior de las Fuerzas Armadas* (ESFAS). En estos casos se hace especialmente útil el desarrollo de las siglas y acrónimos, al tratarse de secciones y departamentos más especializados y menos conocidos por el público general que pueda acercarse a la página.

A propósito de la construcción de la identidad y la legitimación de la institución, vemos que estas se alcanzan a través de la presentación de su trayectoria histórica, su vinculación con universidades (en relación con la investigación y la transferencia del conocimiento) y su papel fundamental en la formación de altos mandos militares. Para ello, se destacan actividades, publicaciones y colaboraciones académicas como prueba de su relevancia.

## 4.2. El Departamento de Seguridad Nacional (DSN)

El DSN depende directamente del Gabinete de la Presidencia del Gobierno y se encarga de asesorar al Presidente del Gobierno en todo lo relacionado con la seguridad nacional. El DSN también «desarrolla funciones en el ámbito de la gestión de las situaciones de crisis (...) que comporten la toma de decisión en el nivel político-estratégico»[23]. Las tres áreas de actuación preferentes del DSN son: la gestión de crisis, la promoción de una cultura de seguridad nacional y el trazado de los riesgos y amenazas a la seguridad nacional.

23. https://www.dsn.gob.es/es/estructuras-de-seguridad-nacional/departamento-seguridad-nacional

La respuesta y la gestión ante posibles crisis resulta fundamental en el mundo actual y sus imprevisibles y súbitos cambios geopolíticos. El DSN basa el modelo de gestión de crisis en el concepto de *resiliencia*, que «incorpora tanto la coordinación entre todas las Administraciones públicas (estatal, autonómica y local), como entre los ministerios, el sector privado y científico y la sociedad civil». Como podemos observar, la sociedad civil está presente en sus planes, y esto implica la necesidad de su conocimiento por parte de esta.

La promoción de la cultura de seguridad nacional, por su parte, está encaminada a favorecer una implicación activa de los ciudadanos, lo cual supone que «el Gobierno deberá poner en marcha acciones y planes que tengan por objeto aumentar el conocimiento y la sensibilización de la sociedad acerca de los requerimientos de la Seguridad Nacional»[24]. Para ello, el Consejo de Ministros aprobó el 25 de mayo de 2021 el *Plan Integral de Cultura de Seguridad Nacional*.

La organización macroestructural del portal web del DSN responde a una estructura dinámica y noticiosa, con titulares actualizados, enlaces a informes y secciones sobre amenazas y riesgos globales. Tiene cuatro secciones principales: Estructuras de Seguridad Nacional, Nuestras áreas de actuación, Publicaciones y Actualidad. En este apartado, la información está orientada a la acción y la actualidad, como en el acceso a la Sala de prensa, donde se pueden encontrar noticias relacionadas con cuestiones que afectan a la seguridad nacional como, por ejemplo, la Operación de Paso del Estrecho -OPE- (en época estival, de tránsito de vehículos en el Estrecho de Gibraltar). La ciudadanía también se puede informar de fuentes oficiales sobre la actualidad de última hora en conflictos como el de Rusia-Ucrania, Oriente Próximo o la situación en Afganistán. La posibilidad de consultar estas fuentes oficiales es una de las principales herramientas en la lucha contra los bulos y la desinformación que se extienden en las redes sociales, como ya hemos comentado.

Por otro lado, la estructura uniforme de algunas secciones ayuda al lector del portal a acceder a la información de una manera ordenada y sistemática. Así, en relación con los Comités especializados, que forman parte de la sección de Estructuras de Seguridad Nacional, la presentación de los contenidos se realiza mediante un esquema fijo de preguntas: Qué es, Quién lo integra, Cada cuánto se reúnen, Para qué sirve y Funciones.

En relación con el registro lingüístico, se emplea un registro formal, pero cercano al ciudadano, con titulares breves y directos, teniendo en cuenta el carácter informativo y gubernamental del portal, con un enfoque orientado a la actualidad, en la sección que constituye su apartado principal. Al

24. https://www.dsn.gob.es/index.php/es/nuestras-areas-de-actuacion/cultura-de-seguridad-nacional

igual que en la página del CESEDEN, encontramos términos especializados como *amenazas híbridas*, *resiliencia nacional* o *comités especializados*. Es muy destacable la corrección formal de los textos y la ausencia de erratas y errores de tipo ortográfico a los que, desgraciadamente, nos tienen acostumbrados hoy los medios de comunicación tanto tradicionales como digitales.

## 4.3. El Centro Nacional de Inteligencia (CNI)

«El CNI es el Servicio de Inteligencia de España. Su naturaleza y las misiones que tiene encomendadas lo configuran como organismo público, adscrito al Ministerio de Defensa, con personalidad jurídica propia y con la plena capacidad de obrar que le otorga la ley»[25]. Se trata, por tanto, de un organismo nacional, de carácter estratégico, especializado en la obtención y análisis de informaciones relevantes para la seguridad de España. Existen otros Servicios de Inteligencia e Información del Estado, pero el CNI está amparado por una ley reguladora y una ley orgánica, está sujeto a un sistema propio de control parlamentario, tiene competencia en materia de Contrainteligencia y la Inteligencia que elabora posee un carácter estratégico ya que «coadyuva al proceso de toma de decisiones al más alto nivel, el del Gobierno»[26].

Su portal web ha sido renovado recientemente, a finales del mes de julio de 2025, por lo que presenta una interfaz más moderna, interactiva y actualizada que la que ofrecía hasta esa fecha. Su imagen corporativa busca, con ese proceso de modernización, acercarse más a la ciudadanía y mostrarse como un organismo actual, en consonancia con los tiempos. Por tanto, el cambio es mucho más que un cambio de imagen corporativa al tratarse del principal canal de presentación de la institución ante los ciudadanos. De hecho, en su página de inicio se han destacado solo dos mensajes: la llamada a los ciudadanos que quieran trabajar en el centro, *Trabaja con nosotros*; y su lema, *Nuestra fuerza es la inteligencia*, que combina de manera positiva en una misma realidad dos conceptos que en el habla común suelen aparecer como antónimos: fuerza e inteligencia.

Así pues, los principales objetivos del nuevo diseño de la página web son: potenciar el reclutamiento de nuevos miembros, fomentar la colaboración ciudadana en materia de seguridad, modernizar la imagen institucional y y reforzar la transparencia y la comunicación pública del CNI con y hacia la ciudadanía[27].

25. CENTRO NACIONAL DE INTELIGENCIA, *Razón de ser*, Ministerio de Defensa, 2022, pág. 10.

26. *Ibid.,* pág. 15.

27. https://www.eldebate.com/espana/20250729/cni-lanza-nueva-web-potenciar-reclutamiento-colaboracion-ciudadana_320059.html

En cuanto a la macroestructura de la página web, uno de los primeros elementos que llama la atención es la incorporación de mensajes multimedia, como vídeos explicativos de las funciones del CNI o recursos gráficos atractivos como líneas del tiempo, para dar a conocer la historia del centro. Un detalle interesante del diseño en la nueva página del CNI es su claridad y su limpieza, incluso «se ha atrevido» a actualizar sus siglas en minúscula, *cni* en vez de *CNI*, con un claro objetivo de empleo de un registro más coloquial.

El tono de la web es cercano, emocional e incorpora lemas de carácter motivacional como *Esto no es un trabajo, es una forma de vivir*, mostrando un estilo comunicativo directo centrado en el factor humano a través de sus tres principios fundamentales: servicio, verdad y futuro.

## 5. Conclusiones

La comunicación estratégica resulta fundamental para los organismos e instituciones oficiales encargados de la seguridad, defensa e inteligencia nacionales. En este trabajo hemos revisado algunos de los conceptos básicos de estos campos y hemos planteado el análisis y la comparación, desde lo comunicativo y lo lingüístico, de tres portales web: el del CESEDEN, el del DSN y el del CNI.

En líneas generales, el CNI ha apostado por un tipo de narrativa más visual en su reciente renovación, con incorporación de elementos gráficos atractivos como vídeos o líneas de tiempo -recursos multimedia-, mientras que la web del DSN tiene una presentación más técnica, centrada en la información objetiva sobre sus funciones y sus órganos de trabajo, con un diseño más sobrio. Por su parte, el CESEDEN, en tanto centro de estudios oficiales de defensa, tiene un público objetivo más profesionalizado, como potenciales candidatos de las Fuerzas Armadas, investigadores o estudiantes de posgrado, y esto se refleja en la mayor sobriedad gráfica y lingüística de su portal, al orientarse más a la especialización y la investigación en defensa.

La modernización en la página del CNI se aprecia también en una búsqueda más evidente de apelación al ciudadano (mediante enlaces), con el uso de tiempos verbales -imperativos- en segunda persona: *trabaja*, *colabora*, etc. La interactividad está presente, por tanto, tanto en el botón de *Trabaja con nosotros*, como en el formulario que promueve la colaboración ciudadana. Podríamos decir que, en líneas generales, la web del CNI está diseñada para acercarse más a la ciudadanía y la del DSN busca ofrecer transparencia oficial y acceso a documentos oficiales, por eso, por ejemplo, se encuentran más documentos en formato *pdf*. Por su parte, la web del CESEDEN está más pensada para profesionales e investigadores de los ámbitos de la defensa, la seguridad y la inteligencia.

# BIBLIOGRAFÍA

**CENTRO NACIONAL DE INTELIGENCIA**, *Razón de ser*, Ministerio de Defensa, 2022.

**Esteban Navarro, M. A.**, *Glosario de Inteligencia*, Madrid: Servicio de Publicaciones del Ministerio de Defensa de España, 2007.

**Gallardo-Paúls, B.**, «Riesgos de la comunicación de riesgo: un modelo discursivo para la comunicación de riesgo en emergencias», en *Círculo de Lingüística Aplicada a la Comunicación*, 88, 2021.

**MINISTERIO DE DEFENSA**, *Directiva de la Ministra de Defensa sobre Comunicación Estratégica*, 2017.

**Molina, I.**, *Conceptos fundamentales de Ciencia Política*, Alianza Editorial, Madrid, 1998.

**Moréu Munáiz, F.**, «Evolución de la cultura de defensa en la última década», en *Arbor, Ciencia, Pensamiento y Cultura* 190 (765), 2014.

**Moya Hernández, G.**, «El lenguaje militar. Tabú, eufemismo y disfemismo», en *Revista Tonos digital* 1, 2001.

**ORGANIZACIÓN PANAMERICANA DE LA SALUD**, «Gestión de la información y comunicación en emergencias y desastres: guía para equipos de respuesta», Organización Regional de Panamá, 2009.

**Pinilla-Gómez, R.**, «Análisis del discurso, poder y guerra de informaciones: el lenguaje y la comunicación en la invasión rusa de Ucrania», en *El discurso como herramienta de control social*, 2023, Peter Lang.

**PRESIDENCIA DE GOBIERNO**, *Directiva de Defensa Nacional,* 2020.

**Sánchez Benítez, S.**, *Documento de Opinión IEEE 21/2011. La comunicación estratégica como política pública*, Instituto Español de Estudios Estratégicos, 2011.

**Sansó-Rubert, D.**, **Pulido-Gragera, J.**, «Cultura de inteligencia y sociedad», en *URVIO. Revista Latinoamericana De Estudios De Seguridad*, 34, 2022.

**Santiago Marín, J. M.**, et al., *Documento de Opinión IEEE 75/2024. Pedagogía de la cultura de la defensa*, Instituto Español de Estudios Estratégicos, 2024.

# VENTAJAS E INCONVENIENTES EN EL USO DE FUENTES PARA EL ANÁLISIS DE LA PIRATERÍA MARÍTIMA

**Fernando Ibáñez Gómez**

*Profesor Doctor de la Universidad a Distancia de Madrid (UDIMA) y del Campus Internacional para la Seguridad y la Defensa (CISDE)*

## 1. Introducción

El uso de fuentes confiables por parte de los analistas de inteligencia es un factor crítico para desarrollar un informe que tenga un nivel de rigor suficiente y que pueda resultar útil para la toma de decisiones. En el caso de la piratería marítima hemos asistido en los últimos años a un incremento notable de fuentes, tanto de organismos públicos[1] como también privados, que han venido, en ocasiones, a favorecer, y en otras a complicar, la labor del analista que se enfrenta al reto de saber qué ocurre en los mares y océanos afectados por esta actividad. Es habitual que las distintas fuentes no coincidan en el número de ataques que se producen en cada región afectada por la piratería. En ocasiones, discrepan en la hora y localización exacta del incidente o duplican ataques, lo que acaba generando confusión al analista. Tampoco se ponen siempre de acuerdo a la hora de denominar cada tipo de ataque o establecer la delimitación geográfica de las regiones donde se producen.

El objetivo de este artículo es analizar las fuentes más relevantes de las que dispone el analista para hacer frente a su labor, así como determinar las ventajas e inconvenientes de cada una de ellas, con el fin de evaluar cuáles son, en el momento presente, las que muestran un mayor rigor a la hora de tratar el fenómeno de la piratería marítima.

1. En estos organismos públicos incluimos agencias navales internacionalmente reconocidas y que cuentan con una recomendación expresa por parte de las asociaciones globales del transporte marítimo y pesquero de altura.

## 2. Una definición de piratería no siempre compartida

Desde el punto de vista legal, el delito de piratería marítima viene regulado en la Convención de las Naciones Unidas sobre el Derecho del Mar (CONVEMAR) de 1982. Allí se define como un acto de violencia cometido con fines privados en alta mar (o en un lugar no sometido a la jurisdicción de ningún Estado) por la tripulación o pasajeros de un buque o una aeronave contra otro buque o aeronave[2].

¿Y cuando ocurre en una zona sometida a la jurisdicción de un Estado? En ese caso no hablamos de actos de piratería, sino de robos a mano armada en el mar. Este último delito viene recogido en la Resolución A1025 (26) de la Organización Marítima Internacional, donde lo define como un acto ilícito de violencia cometido con fines privados contra un buque, o contra las personas o bienes a bordo, en aguas interiores, aguas archipelágicas o el mar territorial de un Estado[3].

El Centro de Información sobre Piratería de la Oficina Marítima Internacional (*International Maritime Bureau Piracy Reporting Center*, en adelante IMB) monitoriza ataques piratas a nivel global desde 1992. Está integrado en la Cámara de Comercio Internacional, una entidad privada establecida en 1981 para luchar contra el fraude y los delitos marítimos. Para este organismo el elemento decisorio para calificar un acto como piratería es el hecho delictivo en sí, independientemente del lugar en que acontezca. Por ello, define la piratería y el robo a mano armada como «acto de abordaje o intento de abordaje con la intención aparente de cometer un robo o cualquier otro delito y con la intención aparente o la capacidad de usar la fuerza para ello». Como explica en sus informes, recoge todos los actos que se realicen, se encuentre el barco atracado, fondeado o en alta mar, aunque excluye de sus estadísticas los pequeños robos, salvo que los asaltantes se encuentren armados[4]. Este ya es un aspecto diferencial importante. Como vemos, este organismo no asume la definición de la CONVEMAR y plantea una propia. Por lo tanto, en el listado de incidentes que muestre el IMB aparecerán mezclados delitos que son diferentes según la CONVEMAR. Y, por ello, si las bases de datos de otros organismos sí distinguen actos piratas de robos a mano armada, lógicamente, las estadísticas no podrán coincidir con las que reporte el IMB.

2. NACIONES UNIDAS (1982), *Convención de las Naciones Unidas sobre el Derecho del Mar*, 1982.

3. ORGANIZACIÓN MARÍTIMA INTERNACIONAL, *Código de prácticas para la investigación de los delitos de piratería y robo a mano armada perpetrados contra los buques*, 2009.

4. INTERNATIONAL MARITIME BUREAU, *Piracy and armed robberies against ships. 2006 annual report*, 2006.

# 3. Fuentes para el análisis de la piratería marítima

Como decíamos en la introducción, el número de fuentes que reportan actos de piratería y robo a mano armada en el mar ha ido aumentando en los últimos años, a la vez que se creaban nuevos organismos y empresas para reportar y analizar este tipo de incidentes. En este apartado vamos a citar todos los que existen en el momento de escribir estas líneas (febrero de 2025). El requisito que exigimos para que formen parte de este análisis es que reporten los incidentes con información suficiente para que el analista pueda identificar el *modus operandi* de los atacantes con datos como fecha, hora y lugar del ataque, tipo de barco atacado y que incluya una narración de los hechos que permita identificar otros datos de interés como el número de asaltantes, las armas que portaban, las contramedidas tomadas desde el barco atacado y el resultado del incidente (robo, secuestro, etc.).

Como se verá, los centros que vamos a analizar son de diverso tipo tanto por su ámbito espacial (algunos aportan incidentes solamente para una región, otros para todo el planeta) como por su carácter público (oficial) o privado. En primer lugar, analizaremos los organismos de ámbito público que reportan incidentes a nivel global; en segundo lugar, los de ámbito privado y, por último, los organismos regionales (todos ellos de carácter público) que centran sus análisis en una región determinada. Por último, veremos algunos centros que, aunque no cumplen los requisitos expuestos, pueden aportar información complementaria útil para el analista.

## 3.1. Centros globales de carácter público

### 3.1.1. International Maritime Organization

La Organización Marítima Internacional (en adelante IMO, por sus siglas en inglés) es la agencia de Naciones Unidas responsable de la seguridad y protección de la navegación y de prevenir la contaminación del mar por los buques. Su página web incluye diversos documentos relacionados con sus distintas áreas de actuación. En el ámbito concreto de la seguridad marítima abarca aspectos como la seguridad portuaria, la piratería, el embarque de vigilantes privados armados, la ciberseguridad, las acciones contraterroristas, el narcotráfico, la presencia de polizones, la construcción de capacidades en diferentes regiones, etc.

Respecto a la piratería y el robo a mano armada en el mar, la IMO publica desde 1982 informes a partir de los datos facilitados por los Gobiernos miembros de la organización y otros organismos competentes como, por ejemplo, el IMB o asociaciones de la industria naviera. Desde 2002, sus informes mensuales y anuales clasifican por separado los actos de piratería y robos a mano armada en el mar.

Los informes incluyen los nombres y descripción de los buques atacados, la posición, fecha y hora de los incidentes, las consecuencias para la tripulación, el buque o la carga, y las medidas adoptadas por la tripulación y las autoridades costeras (este último dato es de interés para conocer las capacidades de respuesta de las fuerzas militares o guardacostas de los países afectados)[5].

### 3.1.2. Maritime Information Cooperation & Awareness Center

El *Maritime Information Cooperation & Awareness Center* (en adelante, Centro MICA) es un organismo francés, con base en Brest, que funciona desde 2016 y es gestionado por una treintena de personas pertenecientes a la Marina francesa y a otros países (España, Bélgica, Portugal). Cumple básicamente dos funciones: identificar y analizar incidentes relacionados con la navegación marítima a nivel global 7 días a la semana, 24 horas al día; y proporcionar a los buques y a sus armadores información sobre zonas marítimas de riesgo, alertas en caso de incidente, evaluaciones de seguridad, etc. En caso de alerta de piratería, mantiene contacto directo con el buque asaltado, avisa a los buques que se encuentran en las proximidades, informa a los centros pertinentes con el fin de coordinar una intervención y realiza una retroalimentación posterior a la alerta.

El Centro MICA establece cuatro tipos de incidentes:

a) Barco pirateado: incidente en el que los atacantes abordan un buque y logran hacerse con el control del mismo o de la tripulación.

b) Ataque: los atacantes llevan a cabo una acción contra el buque sin conseguir abordarlo; o bien abordan el barco con la intención de apoderarse de él o de su tripulación, pero no lo consiguen.

c) Intento: incidente con clara intención de llevar a cabo un ataque en el que los autores apuntaron sus armas hacia el buque, se observó la presencia del equipo necesario para el abordaje (escalera, ganchos) sin que hayan sido utilizados; o se observaron movimientos sospechosos.

d) Robo o intento de robo con o sin violencia: en aguas territoriales (para diferenciarlo de un acto de piratería, de acuerdo con la CONVEMAR).

El Centro MICA viene publicando informes anuales sobre piratería y robo a mano armada en el mar desde el año 2019 en los que realiza un análisis estadístico de los incidentes de este tipo en todo el mundo y por regiones[6]. Las

5. Los informes pueden consultarse en el siguiente enlace electrónico: https://www.imo.org/en/OurWork/Security/Pages/Piracy-Reports-Default.aspx

6. Pueden descargarse del siguiente enlace: https://www.mica-center.org/en/publications-2/

cinco regiones analizadas son el golfo de Guinea, las Américas (incluyendo el Caribe), el océano Índico, Europa y, por último, agrupa en una sola región el sudeste asiático y el océano Pacífico. También proporciona información de cada suceso reseñando fecha y hora, tipo de incidente, objetivo, localización y realiza una descripción breve del mismo. El centro recopila los datos a partir de fuentes internas y externas, como países socios, otros operadores marítimos, agencias y medios de comunicación.

Desde su informe anual de 2023 se ha visto obligado a incluir una nueva categoría de incidentes (no relacionados con la piratería y el robo a mano armada) bajo el epígrafe extensión de un conflicto armado en el mar, que hace referencia a un conflicto en tierra que está impactando en los buques mercantes o en los puertos (en forma de acoso, ataque de drones, etc.). En dicha categoría se recogen los incidentes provocados por los hutíes en Yemen desde noviembre de 2023 y que están afectando a la navegación por el golfo de Adén y el mar Rojo[7].

## 3.2. Centros globales de carácter privado

### 3.2.1. International Maritime Bureau Piracy Reporting Center

El Centro de Información sobre Piratería de la Oficina Marítima Internacional, ya citado en el apartado 2, tiene su sede en Kuala Lumpur (la capital de Malasia). Su intención fue convertirse en el único centro al que todos los barcos que sufrieran un ataque reportaran el suceso con el fin de que contactara inmediatamente con las agencias y fuerzas locales para que prestasen asistencia al buque atacado, además de informar a los barcos que se encontrasen en las proximidades del lugar. También estaba entre sus funciones informar a la Organización Marítima Internacional respecto a los incidentes que se producen para disponer de una información actualizada.

Los informes del IMB son una de las bases de datos tradicionales porque lleva más de treinta años realizando informes trimestrales (en su web aparecen como *Quarterly*) y anuales (*Annual*) muy completos (casi 100 páginas), con tablas, gráficos y análisis de tendencias. Además, proporciona un informe detallado de cada incidente, que incluye la fecha y hora, el nombre y tipo de barco, el pabellón que enarbola, el número IMO[8], la posición en la que

7. En febrero de 2024 y a raíz de los ataques de los hutíes, se creó el Joint Maritime Information Center, un centro británico que informa de los incidentes provocados por dicho grupo. Sus informes semanales y estadísticas mensuales pueden consultarse en el siguiente enlace: https://www.ukmto.org/partner-products/jmic-products

8. La Organización Marítima Internacional otorga un número permanente a un buque para identificarlo, de forma que, aunque cambie de nombre o de pabellón bajo el cual navega, su número seguirá siendo el mismo. Por eso, se conoce como número IMO.

se encontraba en el momento del ataque y una narración sobre lo sucedido. Toda esta información permite al analista identificar la forma de actuación de los asaltantes (cuándo se suele producir un ataque, cuántos atacantes lo protagonizan, qué tipo de barcos sufren los ataques, en qué lugares...), así como la evolución de los ataques en las diferentes regiones. También resulta muy interesante su mapa de piratería en directo, que actualiza periódicamente, y recoge los incidentes que se producen a nivel global[9].

Este centro diferencia cinco tipos de incidentes mediante una muestra de colores: ataques intentados (en amarillo), en los que los asaltantes se aproximan a un barco con intención probablemente de asaltarlo, pero no lo logran; abordajes (en naranja), en los que los atacantes consiguen acceder al buque; secuestros (en rojo), si los asaltantes no solo acceden al buque, sino que se hacen con el control del mismo a costa del capitán y la tripulación; tiroteado (en azul) si el barco sufre disparos de los atacantes mientras intentan acceder al mismo; y, por último, aproximación sospechosa (en morado), si el buque sufre la aproximación de una embarcación sospechosa, si bien no se constata una intención de acceder al mismo.

Quizás este organismo ha sido considerado durante mucho tiempo por la comunidad académica como la fuente más fiable, y también la más utilizada, por la escasez de fuentes abiertas. El problema es que, de un tiempo a esta parte, este centro ya ha dejado de ser el único punto de contacto al que reportan los barcos que sufren un asalto o intento de asalto por parte de piratas y ladrones. Y eso ha sido así aunque el Código de Mejores Prácticas (BMP, por sus siglas en inglés[10]), editado por asociaciones globales del sector marítimo, recomienda que se le incluya como destinatario de informes de incidentes remitidos por buques. La aparición de nuevos organismos ha derivado en que parte de los ataques ya no se reporten a este centro. Y eso ha hecho que en los últimos años sus informes no permitan al analista disponer de toda la información necesaria para tener un conocimiento suficiente de lo que está ocurriendo ahí fuera, lo que obliga a cotejar con otras fuentes.

### 3.2.2. Consultoras de seguridad privada

Existen diversas consultoras de seguridad marítima a nivel global, algunas de las cuales no solo disponen de servicios de análisis de riesgos (por

9. Puede verse en el siguiente enlace: https://icc-ccs.org/map/

10. El documento titulado *Best Management Practices to Deter Piracy and Enhance Maritime Security in the Red Sea, Gulf of Aden, Indian Ocean and Arabian Sea* recoge una serie de recomendaciones y medidas de protección para ayudar a los buques y pesqueros a prevenir y mitigar los riesgos de piratería y de otras amenazas a la seguridad marítima en áreas de alto riesgo. Desde el año 2009 se han publicado cinco versiones del mismo para adaptarse a la evolución de la amenaza. Puede decargarse la última versión en el siguiente enlace electrónico: https://www.ics-shipping.org/wp-content/uploads/2020/08/bmp5-hi-res-min.pdf

ejemplo, la danesa *Risk Intelligence*), sino que incluso ofrecen protección mediante equipos armados de seguridad privada en zonas de riesgo (caso de las británicas *Ambrey* y *EOS Risk*). Dado que se trata de empresas privadas, lógicamente los informes que ofrecen son de pago.

Una que ha demostrado disponer de información de primera mano es la plataforma *Maritime Analysis & Risk Evaluation* (MARE). Según informan en su página de LinkedIn, tiene su sede en Riano (Italia), aunque el teléfono de contacto que ofrece en su web tiene prefijo de Reino Unido. Esta compañía privada pretende aportar un plus de análisis frente a otro tipo de bases de datos existentes para lo que ha creado su propia tecnología desde cero. Se ha especializado en identificar, evaluar y monitorizar en tiempo real amenazas a la seguridad marítima relacionadas con la piratería, el terrorismo o el contrabando. El suscriptor recibe alertas y análisis en profundidad de cada uno de los incidentes reportados.

## 3.3. Centros regionales de carácter público

En este apartado vamos a analizar cuatro centros: dos de ellos se ocupan de la región del Índico, uno del golfo de Guinea y otro del Sudeste asiático.

### 3.3.1. United Kingdom Marine Trade Operations

La oficina de UKMTO (*United Kingdom Marine Trade Operations*) se puso en marcha a finales del año 2001 en Dubái por el Reino Unido a raíz de los atentados del 11 de septiembre contra Estados Unidos. Este organismo se ha centrado en la piratería marítima desde 2007, a raíz del enorme auge de las acciones de los piratas somalíes en el océano Índico occidental y sirve de enlace entre la industria marítima y las fuerzas militares presentes, una función que recuerda a la del IMB. En su página web publica alertas bajo la denominación *Recent incidents*[11]. También publica informes semanales y trimestrales sobre incidentes piratas en la región del Índico occidental, mar Rojo y golfo Pérsico, que abarcan su zona de notificación voluntaria (véase la carta MSC 6099[12]). Recopila su información de diversas fuentes, entre ellas, lógicamente, la propia UKMTO, así como otras organizaciones de seguridad marítima de la región.

La UKMTO gestiona un Sistema de Notificación Voluntaria (*Voluntary Reporting Scheme* o VRS). Los barcos, una vez que entran en la zona de registro voluntario (véase mapa de la anterior nota a pie de página), son invitados

11. Pueden visualizarse en la siguiente web: https://www.ukmto.org/recent-incidents

12. Esa zona viene señalada en el mapa que puede visualizarse en este enlace: https://cd.royalnavy.mod.uk/-/media/ukmto/charts/q6099.pdf?rev=ea3de0edd2ee432cbae163b36a49f9d6&hash=8D41980116B444BE21920085AD7B80EB

a enviar informes diarios, preferiblemente por correo electrónico, a las 08.00 UTC (hora 0, del meridiano de Greenwich) con información como su posición, rumbo, velocidad y fecha prevista de llegada a su siguiente puerto. Esa información permite rastrear la situación de los buques y es enviada a los cuarteles de los efectivos militares desplegados en la zona.

La gran ventaja de los informes de la UKMTO es que se actualizan con frecuencia. Y son especialmente útiles sus alertas (*Warnings*) que suelen publicarse con celeridad desde el momento en que se produce el incidente. Sin embargo, no suele emitir alertas cuando se encuentran involucrados pesqueros, debido quizás a que éstos no participan en los sistemas de notificación voluntaria como lo hacen los buques mercantes. Este hecho podría ser relevante para el investigador dado que el uso de pesqueros locales previamente secuestrados (conocidos como *dhow*s) como buques nodriza por parte de grupos de acción pirata es una práctica habitual en el Cuerno de África.

### 3.3.2. Maritime Security Centre-Horn of Africa y Maritime Security Centre Indian Ocean

El Centro de Seguridad Marítima-Cuerno de África (en adelante, MSC-HOA por sus siglas en inglés) fue creado por la Unión Europea como parte de su iniciativa para luchar contra la piratería marítima en aguas de Somalia y en apoyo a las resoluciones del Consejo de Seguridad de Naciones Unidas 1814, 1816 y 1838[13].

El MSC-HOA, con sede en la localidad francesa de Brest, dispone de una dotación de personal militar y está integrado funcionalmente en el Cuartel General de la operación naval europea EU NAVFOR Atalanta, desplegada desde 2008 para hacer frente a la piratería somalí. Desde la puesta en marcha de la operación ASPIDES de la Unión Europea para afrontar la amenaza de los hutíes, también sirve a la nueva misión con la intención de mantener una única interfaz entre las operaciones de política común de seguridad y defensa de la UE y la comunidad mercante en la región del Índico, mar Rojo y golfo Pérsico.

Su página web ofrece a los armadores y capitanes la posibilidad de registrar sus datos de forma segura, actualizar las posiciones de sus buques y recibir información y orientación destinadas a reducir el riesgo de ataques piratas. También ofrece inteligencia marítima sobre la piratería, las tácticas de los piratas y cómo actuar cuando un buque es secuestrado. Sus alertas (a las que se accede solo si se ha registrado el buque en su web) son imprescindibles para conocer información casi a tiempo real sobre ataques piratas en

13. Estas resoluciones, aprobadas en el año 2008, básicamente autorizaban a los buques de guerra la entrada en las aguas territoriales somalíes con el fin de perseguir a los piratas, siempre que se dispusiera de la autorización del Gobierno Federal de Transición somalí. Y exhortaban a todos los Estados a que desplegasen «buques de guerra y aeronaves militares» para luchar contra la piratería.

la zona de operaciones. Tiene una base de datos sobre incidentes de seguridad marítima. Si bien sus informes trimestrales no son de acceso público, sí que publica de forma abierta documentos actualizados sobre la situación de la piratería en la región, denominados *Update on the piracy threat off the coast of Somalia*, así como de la amenaza de ataques al tráfico tras la crisis provocada por los hutíes.

En los primeros días de diciembre de 2024 cambió su denominación por *Maritime Security Centre Indian Ocean* (MSCIO). Tras unos días en los que las webs de ambos organismos permanecieron activas, la antigua dejó de estar disponible[14]. Sin embargo, para finales de febrero de 2025 la nueva web todavía anunciaba que se encontraba **«**en proceso de actualización y mejora**»** y, por ejemplo, el sistema de alertas no funcionaba aún. De hecho, la primera alerta como tal fue publicada en mayo de 2025. También sorprende que, a diferencia de lo que ocurría en el portal de MSC-HOA, en la nueva web de MSCIO se publique en abierto el programa de los convoyes[15] establecidos para proteger a los mercantes que atraviesan el golfo de Adén y que gestionan armadas independientes como la china, la japonesa o la paquistaní. Cabe preguntarse si dichos países estarán conformes con que se dé información pública sobre la posición, aunque sea aproximada, de sus unidades navales en la región.

Uno de los objetivos que se decidieron en la 52ª reunión del organismo de coordinación SHADE[16] en diciembre de 2024 fue crear un mismo formato para notificar incidentes o para informar de la situación del barco independientemente de si se dirigen a la UKMTO o al MSCIO. Pero, en caso de incidente, la UKMTO actuará como **«**punto primario de contacto e intercambio central de información, compartiéndola rápidamente para permitir una respuesta y un apoyo eficientes y eficaces**»**[17] (este papel como punto primario de

14. Su nueva web es https://mscio.eu

15. Sobre el funcionamiento del sistema de convoyes en el golfo de Adén, véase el documento *Gulf of Aden Internationally Recommended Transit Corridor & Group Transit Explanation* en el siguiente enlace: https://mscio.eu/documents/95/GROUP_TRANSITS_-_2025_MSCIO.pdf

16. Inicialmente, en las reuniones SHADE (*Shared Awareness and Deconfliction*) han estado representadas las operaciones militares desplegadas (de la Unión Europea, de las Fuerzas Marítimas Combinadas, lideradas por Estados Unidos, y en su día también de la OTAN), y los diversos actores que intervienen en la zona de operaciones de los piratas somalíes (marinas de países no pertenecientes a ninguna de las coaliciones internacionales, como Rusia, China, India, Japón, Turquía, etc., así como potencias regionales, países ribereños, asociaciones de pesqueros y de buques mercantes, armadores, industria marítima, empresas de seguros, etc.). Su objetivo es fomentar la coordinación y cooperación en el ámbito de la seguridad marítima y de la lucha contra la piratería somalí.

17. Tal y como se refleja en la VOLUNTARY REPORTING GUIDANCE IN THE INDIAN OCEAN AND RED SEA REGION JANUARY 2025, que puede consultarse en este enlace: https://mscio.eu/documents/100/Voluntary_Reporting_Guidance_in_the_Indian_Ocean_and_Red_Sea_Region.pdf

contacto está reconocido por la industria en las BMP). Estos cambios obligaban a realizar modificaciones en las páginas web de ambos organismos, que esperaban haberse completado en marzo de 2025. Para algunos analistas, la impresión que dan estos cambios es que, en general, la operación Atalanta ha descendido un escalón en favor de la UKMTO.

### 3.3.3. Maritime Domain Awareness for Trade-Gulf of Guinea

En la región del golfo de Guinea existe el *Maritime Domain Awareness for Trade-Gulf of Guinea* (MDAT-GoG), un centro que funciona desde 2016 y que es fruto de la cooperación entre las marinas británica (a través de la UKMTO) y francesa (Centro MICA). No hay que olvidar la influencia de las dos antiguas potencias coloniales en África occidental. Son francófonos estados como Benín, Burkina Faso, Chad, Costa de Marfil, Gabón, Guinea, Mali, Níger, República Centroafricana, República del Congo, República Democrática del Congo, Senegal y Togo. Y son anglófonos Gambia, Ghana, Liberia, Nigeria y Sierra Leona.

De manera similar a como hace la UKMTO en el océano Índico, el MDAT-GoG es el organismo al que deben pedir auxilio los buques que navegan por la región y sufren un ataque pirata. Además, se pretende que, una vez que un buque entre en el área de notificación voluntaria, denominada *Voluntary Reporting Area* (VRA)[18], informe de su posición al centro periódicamente. Se debe enviar un informe inicial y, posteriormente, informes diarios en los que se actualice la posición, el rumbo y la velocidad del barco. Por último, se remite un informe final, una vez se abandone el VRA o se llegue a puerto. También solicita que se envíen informes de cualquier actividad sospechosa o irregular, información que será tratada como confidencial. Asimismo, el MDAT-GoG ejerce de enlace con las fuerzas militares de la región y ofrece a los capitanes de los buques la posibilidad de realizar simulacros y ejercicios que les permitan planificar su navegación por el área. Las dimensiones de la VRA sugieren los relativamente bajos porcentajes de participación en el sistema de notificación voluntaria, que parecen concentrarse principalmente en el golfo de Guinea en sentido estricto (aproximadamente desde cabo Palmas a cabo López)

El MDAT-GoG publica en su página web un mapa con los incidentes reportados (que pueden visualizarse para los últimos 10, 30, 90 ó 365 días) así como informes semanales, mensuales y semestrales donde recoge amplia información sobre los mismos, así como las tendencias de su evolución en los últimos años[19].

18. Puede visualizarse un mapa de la VRA en el siguiente enlace: https://services.data.shom.fr/static/imagettes/NAUTIQUE/PQP_8801CSD_NP_Carte-Surete-Maritime-Golfe-De-Guinee.pdf

19. Pueden descargarse los informes en el siguiente enlace: https://gog-mdat.org/reports

### 3.3.4. The Regional Cooperation Agreement on Combating Piracy and Armed Robbery against Ships in Asia

Específicamente para el caso de la piratería en el Sudeste asiático cabe citar los informes publicados por el Acuerdo regional de cooperación para combatir la piratería y el robo armado contra barcos en Asia (ReCAAP, por sus siglas en inglés). Este acuerdo se puso en marcha en 2006 para coordinar las respuestas de Malasia, Indonesia y Singapur ante el auge experimentado por la piratería en el estrecho de Malaca, mediante el desarrollo de propuestas concretas como, por ejemplo, patrullas conjuntas.

Este organismo establece dos criterios para evaluar los incidentes de piratería. Por un lado, el nivel de violencia ejercida durante el ataque, que mide con tres indicadores: armas utilizadas (cuanto más sofisticada sea el arma utilizada mayor será el nivel de violencia, ya que no es lo mismo usar armas blancas que armas de fuego); el trato que se dispense a la tripulación (varía desde la huida si el atacante es detectado por la tripulación a realizar amenazas o lesiones sobre los mismos, secuestrarlos o incluso provocar su muerte); y el número de atacantes involucrados, dado que se considera que un mayor número de atacantes suele ser propio de organizaciones criminales. El segundo criterio es la pérdida económica sufrida, que incluye el tipo y la cuantía de bienes sustraídos.

A partir de estos dos criterios el ReCAAP establece cuatro categorías de incidentes, de mayor a menor gravedad. En la categoría 1 incluye aquellos que involucran a más de 9 asaltantes, armados con pistolas y cuchillos, y en los que la probabilidad de que los miembros de la tripulación sufran lesiones o violencia física es alta. Desde el punto de vista económico, en este tipo de incidentes el barco suele ser secuestrado o la carga robada. En la categoría 2 los asaltantes suelen ser de 4 a 9 personas, con cuchillos y machetes, y en menos casos con pistolas. Suelen amenazar o retener a la tripulación, pero solo de forma temporal, para hacerse con el dinero o propiedades del barco. La tripulación puede sufrir lesiones o violencia, pero de menor intensidad que en la categoría previa. En los incidentes de categoría 3 los asaltantes suelen ser de 1 a 6 personas, armadas con cuchillos, machetes, palos, bates, etc. Aunque la tripulación puede verse coaccionada, no sufre daños. Y con frecuencia solamente pueden llevarse provisiones o repuestos de motores. Por último, están los incidentes de categoría 4, que involucran a 1-3 personas, con asaltantes no armados y que suelen huir sin conseguir nada cuando son detectados por la tripulación.

El ReCAAP emite informes semanales, mensuales, trimestrales, bianuales, anuales e, incluso, algunos de carácter especial cuando considera oportuno realizar un análisis más profundo de algún tema en concreto[20]. Utiliza diversas fuentes de información para elaborar sus informes: desde su propia red

20. Pueden verse todos los informes publicados por el ReCAAP desde el año 2006 en el siguiente enlace: https://www.recaap.org/reports

hasta los informes de la IMO, *The Information Fusion Center* (del que hablamos en el siguiente punto), las autoridades malasias e indonesias, compañías navieras, armadores, operadores y agentes de buques, y otras fuentes de acceso público.

## 3.4. Centros que aportan información complementaria

### 3.4.1. The Information Fusion Center

El Centro de Fusión de Información (IFC, por sus siglas en inglés) se creó en 2009 y tiene su sede en Changi, siendo gestionado por la marina de Singapur. Realiza informes semanales, mensuales, trimestrales, semestrales y anuales relacionados con diversos delitos del ámbito marítimo: desde la piratería y el robo a mano armada en el mar hasta el terrorismo, pasando por la pesca ilegal, el contrabando, la migración irregular y aspectos medioambientales y de ciberseguridad[21]. Sin embargo, no hace una relación pormenorizada de los incidentes de piratería, como otros organismos públicos que hemos visto previamente (la IMO y el Centro MICA). No obstante, sus análisis de tendencias pueden ser de interés para el analista y le pueden permitir complementar su investigación con la información que aportan este tipo de agencias, que son las que vamos a ver en este apartado.

Para diciembre de 2024 había 26 oficiales de enlace de 20 países desplegados en el IFC y tenía vínculos con 143 socios de 57 países, entre los que se incluyen armadas, guardacostas, agencias marítimas, asociaciones y compañías navieras... Esto permite al IFC incluir en sus informes análisis de organismos públicos como la UKMTO, el Centro de Fusión de Información Marítima de Latinoamérica (con sede en Perú), la marina de Estados Unidos (análisis de los ataques hutíes en el mar Rojo y el golfo de Adén), de Vietnam (sus acciones contra la pesca ilegal), la Agencia Marítima de Malasia (su lucha contra el contrabando), Indonesia (su análisis sobre migración irregular), entre otros. Incluso hay en sus informes aportaciones de consultoras de seguridad privada como *Ambrey*. Todo ello le permite generar información de fuentes muy diversas que aportan interesantes análisis sobre los fenómenos estudiados por cada una de ellas.

### 3.4.2. Information Fusion Centre-Indian Ocean Region

El Centro de Fusión de Información-Región del Océano Índico (IFC-IOR, por sus siglas en inglés) fue establecido por la Marina india en el año 2018 en la localidad de Gurugram, con el fin de promover la seguridad marítima en la

21. Pueden descargarse desde el siguiente enlace electrónico: https://www.ifc.org.sg/ifc2web/app_pages/User/commonv2/pubsProducts.cshtml

región del océano Índico. Este Centro trabaja con socios de 14 países (Australia, Bangladesh, EE. UU., Francia, Italia, Japón, Maldivas, Mauricio, Myanmar, Reino Unido, Seychelles, Singapur, Sri Lanka y Tailandia) y también ha establecido vínculos con más de 50 países, agencias y centros de seguridad marítima.

Al igual que ocurre con el IFC de Singapur, el IFC-IOR indio no solo incluye en sus informes actos de piratería y robo a mano armada en el mar, sino que también analiza otros fenómenos como el contrabando, la pesca ilegal o el tráfico de personas[22].

### 3.4.3. Office of Naval Intelligence

La Oficina de Inteligencia Naval de Estados Unidos (ONI) pertenece a la marina de dicho país y su fin es recopilar, analizar y producir inteligencia marítima para favorecer la toma de decisiones de los responsables. En el ámbito de la piratería, publica unos informes mensuales (eran semanales hasta agosto de 2020) denominados *Worldwide Threat to Shipping*[23]. Entre las fuentes que utiliza para preparar estos informes se encuentran desde organismos ya vistos aquí (como el IMB, la IMO, los centros de la operación Atalanta, el MDAT-GoG, la UKMTO y el ReCAAP) hasta otros pertenecientes a la Administración marítima o la guardia costera norteamericanas, a marinas de otros países, pasando por noticias de medios de comunicación. Por las fuentes utilizadas se trata de unos informes muy fiables para el analista.

## 4. Análisis comparativo de las distintas fuentes

La forma de analizar comparativamente las diferentes fuentes pasa necesariamente por identificar su calidad tanto desde un punto de vista cuantitativo (cuál de ellas ofrece un mayor número de incidentes) como cualitativo (cuál ofrece más información de cada caso), lo que permitirá al analista tener un panorama más próximo a la realidad de los incidentes de piratería y robo a mano armada a nivel global, y realizar un análisis más acertado.

Desde un punto de vista cuantitativo, probablemente los centros oficiales que aportan un mayor número de incidentes en estos momentos son el Centro MICA y la Oficina de Inteligencia Naval norteamericana. Es cierto que, como ya explicamos en otro lugar[24], en ocasiones, la agencia norteameri-

22. Pueden verse sus informes en su página web: https://www.indiannavy.nic.in/ifc-ior/index.html, si bien es cierto que con frecuencia no funciona.

23. Pueden consultarse los publicados desde el año 2018 en el archivo de su web: https://www.oni.navy.mil/ONI-Reports/Shipping-Threat-Reports/Worldwide-Threat-to-Shipping-Report-Archive/

24. Ibáñez, F., *La amenaza de la piratería marítima a la seguridad internacional: el caso de Somalia*. Ministerio de Defensa, 2012, pág. 236.

cana duplica algunos incidentes, dado que le llegan de diferentes fuentes, pero también es evidente que en los últimos años ha realizado un notable esfuerzo para reducir este problema. Por otra parte, diversos estudios parecen confirmar que tanto el IMB como la IMO no son capaces de reportar un número de incidentes similar al de otras fuentes[25]. Esto puede deberse a que los estados no reportan todos los incidentes a la IMO y/o a que algunos buques no incluyen al IMB como destinatario de los informes de incidentes (a pesar de que se recomienda hacerlo en las BMP).

Si bien es cierto el importante papel que ha desempeñado el MSC-HOA en el pasado, también lo es que, ante la reducción de los ataques de piratas somalíes en años recientes, parece haber sufrido una cierta esclerotización. Esto se observó en particular con el resurgimiento de incidentes de piratería en esta región, a finales del año 2023 y en consonancia con el aumento de la inseguridad marítima en el mar Rojo y el golfo de Adén a consecuencia de los ataques de los hutíes contra mercantes y buques de guerra[26].

Por ejemplo, el MSC-HOA no emitió ninguna alerta el 1 de noviembre de 2024 cuando se produjo el secuestro de un pesquero iraní frente a la costa de Somalia, a la altura de Eyl. Sin embargo, otras fuentes sí lo citaban y advertían de que, apenas diez días antes, el 22 de octubre, había salido un grupo pirata desde la localidad somalí de Ceel Huur. Y al día siguiente, 2 de noviembre, ocurría lo mismo. Se producía un nuevo ataque pirata sobre un pesquero a 14 millas al suroeste de Hafun (Somalia) por parte de personas armadas en un esquife. Y, por segunda vez, no se reportaba ninguna alerta en fuentes oficiales. Ese mismo mes, el 27 de noviembre se conoció el secuestro de un pesquero chino por seis piratas somalíes armados con AK 47 a unas 11 millas de la localidad somalí de Garmal. Tampoco se informó en fuentes oficiales del mismo.

Resulta significativo que ni el MSC-HOA ni UKMTO emitieran alerta alguna respecto a estos tres incidentes de noviembre de 2024. ¿Cómo se dieron a conocer? Los tres fueron reportados por fuentes no oficiales, en particular, por la empresa especializada en inteligencia marítima *Maritime Analysis & Risk Evaluation* (MARE) de la que hemos hablado previamente[27]. Y del tercero de ellos también informó, después de MARE, la consultora británica de seguridad *EOS Risk*[28].

---

25. Véase, por ejemplo, el análisis de fuentes para el golfo de Guinea en Ibáñez, F., «Piratería marítima: estado de la cuestión», en *Revista de Pensamiento Estratégico y Seguridad CISDE* 6 (2), 2021, págs. 71-86.

26. El MSC-HOA comenzó a servir también a la operación ASPIDES de la UE, puesta en marcha como consecuencia del surgimiento de la denominada crisis del mar Rojo, provocada por el ataque de los hutíes al tráfico mercante.

27. Su página web es https://marerisk.com/

28. Su responsable, Martin Kelly, informó del incidente del 27 de noviembre en sus redes sociales. Por ejemplo, en su cuenta en X: https://x.com/_MartinKelly_/status/1862390899038183559

Respecto al último de los incidentes, el 2 de diciembre EOS Risk señalaba que la Policía Marítima de la región somalí de Puntlandia[29] había informado el 27 de noviembre que seis piratas armados con fusiles AK47 habían secuestrado un pesquero chino en aguas territoriales somalíes. El 1 de diciembre se dirigió a mar abierto con 40 piratas fuertemente armados a bordo. También informaba que las autoridades de Puntlandia estaban planeando una operación de rescate sobre el buque y su tripulación. Es interesante el comentario con el que acaba el análisis de *Eos Risk*: **«**La exactitud de estos informes sigue siendo cuestionable**»**, dando a entender que, quizás, no confían demasiado en la información que puedan proporcionar las autoridades de la región somalí.

Por su parte desde la plataforma MARE se aportaban más detalles de los que suministraba *EOS Risk*. Se afirmaba que el ataque ocurrió cuando el pesquero entraba en aguas somalíes. Sobre el número de atacantes, aunque los informes iniciales hablaban de seis piratas, señalaba que otras fuentes sugerían que habían sido hasta diez. Analizaba que el incidente podía guardar relación con las quejas de pescadores somalíes por la acción de pesqueros extranjeros. Y advertía de que el pesquero podría ser usado como buque nodriza desde el que realizar nuevos ataques.

Por fin, el 5 de diciembre, ocho días después del incidente, se emitía una alerta desde el MSC-HOA informando que un atunero chino había sido secuestrado en aguas territoriales somalíes. Y que la fragata española Santa María, desplegada en la operación Atalanta, había detectado el 4 de diciembre al pesquero cerca de la localidad de Eyl y estaba monitorizando la situación.

Algo similar ocurrió el 17 de febrero de 2025 cuando el Centro MICA comunicó que un pesquero con bandera yemení había sido secuestrado frente a la costa somalí y probablemente con la intención de usarlo como buque nodriza desde el que secuestrar otros buques. Este incidente no fue reportado ni por el MSCIO ni por UKMTO.

Sea como fuere, en nuestra opinión, el hecho de que no se emitieran alertas por parte del MSC-HOA/MSCIO ni por la UKMTO resulta preocupante. No solo porque las alertas suponen un elemento imprescindible para advertir a los mercantes de que eviten aproximarse a una zona de riesgo en un momento oportuno, sino porque, sin ellas, no es posible tener una visión real de lo que está ocurriendo en la zona de operaciones de los piratas. Esto afecta no solo a la misión principal de la operación Atalanta, que es proteger a los buques vulnerables que navegan por la región, algo difícil de realizar si no se dispone

29. Puntlandia es una región somalí que funciona de forma autónoma y que fue tristemente famosa por albergar buena parte de las bases desde las que los piratas somalíes comenzaron a lanzar sus ataques a principios de siglo. Su Policía Marítima fue puesta en marcha en 2010 financiada por Emiratos Árabes Unidos y por Erik Prince, fundador de la conocida empresa de seguridad privada Blackwater. Sus éxitos a la hora de arrestar a pesqueros que faenaban ilegalmente en sus aguas fomentaron que la Unión Europea financiara su formación a partir del año 2014. Se ha convertido en una de las escasas fuerzas existentes en Somalia capaz de desarrollar unas mínimas funciones de guardia costera.

de un panorama completo de lo que sucede, sino también a la flota mercante y pesquera, dado que impide realizar una evaluación apropiada del riesgo que se corre. En todo caso, más vale tarde que nunca.

Curiosamente, el 5 de diciembre de 2024 el MSC-HOA emitió otra alerta referida a un problema que había tenido un carguero y había derivado en una inundación dentro del barco. Se informaba de que la tripulación había sido rescatada por efectivos de un buque de guerra francés. Lo sorprendente de esta alerta es que no guarda ninguna relación con el ámbito de protección marítima (*security* en inglés, *sureté* en francés), que es la labor que desempeña el Centro, sino que es más propia de un accidente (*safety* en inglés, *sécurité* en francés). Es más, cabe preguntarse si debe emitirse una alerta por un suceso que no afecta a la protección del tráfico mercante en general.

También sorprende que el cambio de la plataforma del MSC-HOA por la nueva del MSCIO derivara en la pérdida durante meses de las alertas como fuente de información crítica en el momento que un barco sufre un ataque.

Para el estudio de los incidentes en el sudeste asiático tanto el Centro MICA como el ReCAAP confirman un número de ataques similar, en torno al centenar de incidentes en 2024 (103 según el primero y 107 según el segundo). Sin embargo, ambos organismos coinciden en 76 incidentes: el Centro MICA aporta 27 casos de los que no informa el ReCAAP, y éste hace lo mismo para 31 incidentes que no reporta el primero. Por lo tanto, el uso de ambas fuentes nos permite obtener un total de 134 ataques (un 25 % más de casos que la media de ambas).

Si analizamos la región del golfo de Guinea, el Centro MICA reportó un total de 26 incidentes en el año 2024, mientras que el MDAT-GoG reportó 23. Sin embargo, si cotejamos ambas bases de datos podemos sumar un total de 31 incidentes en dicha zona (un 26 % más de casos).

Como se ve, el cotejo de fuentes puede dar al analista bastante más información que el uso exclusivo de una sola base de datos.

## 5. Conclusiones

La ausencia de un sistema de categorización de eventos estándar es un problema para el analista que se enfrenta a la labor de investigar la piratería marítima y el robo a mano armada en el mar. No categorizan de la misma forma los incidentes el IMB o el Centro MICA que UKMTO y el antiguo MSC-HOA, dado que estos últimos dos organismos siguen las definiciones de las BMP[30].

30. Según las BMP, un ataque de piratería puede incluir: el uso de violencia contra el buque o su tripulación, o cualquier intento de usar la violencia; el intento de abordar ilegalmente el buque cuando el capitán sospecha que se trata de piratas; un abordaje real, tanto si consiguen hacerse con el control del buque como si no; y los intentos de superar las medidas de protección mediante el uso de escalas, ganchos o armas contra el barco o dentro del mismo.

En nuestra opinión, el Centro MICA se ha convertido en la mejor fuente pública (y accesible) para analizar incidentes de piratería y robo a mano armada a nivel global, aportando más información y más confiable que, por ejemplo, el IMB o la IMO. Probablemente, esto se debe a que el Centro MICA ha firmado un acuerdo con el MSCIO de la operación Atalanta. Y también al acuerdo entre la Marina británica (a través de UKMTO) y la Armada francesa (vía Centro MICA) para operar el MDAT-GoG, cuyo sistema de notificación voluntaria se gestiona desde el Centro MICA. Esto le permite disponer de más fuentes de información. También da la sensación de que el cambio del MSC-HOA a MSCIO es producto de una mayor influencia francesa en el ámbito de estos centros, aunque sugiere una línea de acción orientada a una proyección más allá del Cuerno de África, reforzando el pretendido papel de «proveedor de seguridad marítima» (más allá de la piratería) que la operación Atalanta incluye en su comunicación estratégica. En este sentido, cabe recordar que la misma operación Atalanta suprimió en el mandato anterior la palabra Somalia de su denominación, por la misma razón aparente.

Para los análisis de los incidentes en el golfo de Guinea o en el sudeste asiático concluimos que conviene cotejar los datos del Centro MICA con los que aportan los centros regionales del MDAT-GoG (para el golfo de Guinea) y del ReCAAP (en el caso del sudeste asiático) para poder enriquecer el análisis.

En el ámbito privado, creemos que la información aportada por MARE parece estar por encima de la media, al menos, respecto a la que hacen pública en las redes sociales otras empresas similares.

## BIBLIOGRAFÍA

**BIMCO, ICS, IGP&I Clubs, INTERTANKO** and **OCIMF**, *BMP5 Best Management Practices to Deter Piracy and Enhance Maritime Security in the Red Sea, Gulf of Aden, Indian Ocean and Arabian Sea*, 2018.

**Ibáñez, F.**, *La amenaza de la piratería marítima a la seguridad internacional: el caso de Somalia*, Ministerio de Defensa, 2012.

**Ibáñez, F.**, «Piratería marítima: estado de la cuestión», en *Revista de Pensamiento Estratégico y Seguridad CISDE,* 6 (2), 2021.

**INFORMATION FUSION CENTRE-INDIAN OCEAN REGION**, *IFC Products*, 2025.

**INTERNATIONAL MARITIME BUREAU**, *Piracy and armed robberies against ships. 2006 annual report*, 2006.

**INTERNATIONAL MARITIME BUREAU**, *IMB Piracy & Armed Robbery Map,* 2025.

**INTERNATIONAL MARITIME ORGANIZATION**, *Piracy reports*, 2025.

**MARITIME SECURITY CENTER INDIAN OCEAN**, *Gulf of Aden Internationally Recommended Transit Corridor & Group Transit Explanation*, 2025

**MARITIME SECURITY CENTER INDIAN OCEAN**, *Voluntary Reporting Guidance In The Indian Ocean And Red Sea Region. January 2025*, 2025.

**MARITIME DOMAIN AWARENESS FOR TRADE — GULF OF GUINEA**, *Reports*, 2025.

**MICA CENTER**, *MICA Center publications*, 2025.

**NACIONES UNIDAS**, *Convención de las Naciones Unidas sobre el Derecho del Mar*, 1982.

**OFFICE OF NAVAL INTELLIGENCE**, *Shipping Report Archive*, 2018.

**ORGANIZACIÓN MARÍTIMA INTERNACIONAL**, *Código de prácticas para la investigación de los delitos de piratería y robo a mano armada perpetrados contra los buques*, 2009.

**RECAAP INFORMATION SHARING CENTRE**, *Reports*, 2025.

**SHOM**, *Carte de Sûreté Maritime. Afrique de l´Ouest. Golfe de Guinée*, 2024.

**UKMTO**, *JMIC products*, 2025.

**UKMOT**, *Recent Incidents*, 2025.

**UK HYDROGRAPHIC OFFICE**, *Maritime Security Chart Red Sea, Gulf of Aden and Arabian Sea Q6099*, 2023.

# PERSPECTIVAS ACTUALES Y FUTURAS DE LOS MÉTODOS DE OBTENCIÓN DE INFORMACIÓN DE LOS SERVICIOS DE INTELIGENCIA PORTUGUESES: LAS INTERCEPTACIONES TELEFÓNICAS Y LOS DATOS DE TRÁFICO

**João Miguel Oliveira Narciso**
*Doctorando en Ciencias Penales*
*University of Coimbra*

## 1. Introducción

Las sociedades contemporáneas, al enfrentarse a una nueva y amplia gama de amenazas, aspiran a un nuevo tipo de respuestas para las que los instrumentos represivos tradicionales se consideran insuficientes e inadecuados. Consciente de esta realidad, el poder estatal, al desplazar su intervención del plano represivo al preventivo, ha encontrado en el refuerzo de los poderes conferidos a los servicios de inteligencia (también conocidos, de forma no tan rigurosa, como «servicios secretos») uno de los medios por excelencia para satisfacer esta creciente demanda de seguridad.

En Portugal, uno de los debates más recurrentes en materia de seguridad es la cuestión del refuerzo de las capacidades operativas de estos servicios, más concretamente el problema de incluir en la lista de medios de actuación del Sistema de Información de la República Portuguesa la realización de escuchas telefónicas y el acceso a datos de tráfico. Se trata de un tema de actualidad, ya que en 2015 y 2019 fue objeto de dos sentencias del Tribunal Constitucional, que consideró que el uso de estos medios restringe el art. 34.4 CRP. Desde entonces, se ha debatido cada vez más la posibilidad de una revisión constitucional de la norma, con el fin de eliminar este obstáculo.

Para abordar correctamente este tema, conviene, en primer lugar, presentar de forma sintética el marco jurídico del Sistema de Información de la República Portuguesa. Una vez expuestas claramente algunas de las

particularidades de su funcionamiento (en particular, lo que diferencia la inteligencia de una investigación desarrollada en la fase de investigación del proceso penal), enumerar los medios legales que actualmente están previstos en la legislación portuguesa. Y, en este contexto, es importante tener en cuenta no solo los medios que están expresamente previstos en la ley, sino también otros cuya posibilidad de utilización se ha planteado y cuestionado.

El acceso a los datos de tráfico y la realización de interceptaciones telefónicas es el tema más debatido y, para analizar adecuadamente este problema, es necesario presentar el debate que se ha planteado, en particular, en relación con los datos de tráfico. En primer lugar, hay que saber si los datos de tráfico están incluidos en el ámbito de protección del derecho a la inviolabilidad de las telecomunicaciones, previsto constitucionalmente en el art. 34.4 CRP. En segundo lugar, si ya es posible, mediante un argumento de similitud entre la actividad de los servicios de inteligencia y la materia del proceso penal, incluir la inteligencia en el ámbito de la restricción prevista por la norma. Dado que el Tribunal Constitucional no ha validado ese acceso, se observará que ya se han presentado proyectos de revisión constitucional para modificar esa norma, por lo que es posible que el tema conozca nuevos desarrollos en el futuro.

## 2. El sistema de información de la República Portuguesa

El Sistema de Información de la República Portuguesa (en adelante, SIRP) se creó en 1984 y, en la actualidad, su funcionamiento se rige esencialmente por dos diplomas legales: el primero es la Ley Marco del Sistema de Información de la República Portuguesa (LQSIRP), Ley n.º 30/84, de 5 de septiembre, y el segundo es la Ley que establece la organización del Secretario General del SIRP, del SIED y del SIS (LOSIRP), Ley n.º 9/2007, de 19 de febrero. Centrándonos en estos dos instrumentos normativos, veamos, en lo que estrictamente interesa a este trabajo, la regulación jurídica del Sistema.

Comenzando por las finalidades que se han atribuido legalmente a los servicios de inteligencia que lo integran, estas son, según la declaración general plasmada en el art. 2.2 LQSIRP, garantizar, en el respeto de la Constitución y la ley, la producción de la información necesaria para la preservación de la seguridad interna y externa, así como la independencia y los intereses nacionales y la unidad e integridad del Estado.

Cabe adelantar, pasando ahora al elenco de órganos, que la coordinación de la actividad de producción de información está, en Portugal, centralizada en el Primer Ministro, que actúa como órgano de dirección política superior del Sistema. En lo que respecta a los organismos responsables de la producción de información, coexisten, dentro de la estructura del SIRP, por un lado,

el Servicio de Información Estratégica de Defensa (SIED), encargado de producir información que contribuya a salvaguardar la independencia nacional, los intereses nacionales y la seguridad exterior del Estado portugués (art. 20 LQSIRP y art. 3.2 LOSIRP). Por otro lado, el Servicio de Información de Seguridad (SIS), que se encarga, a su vez, de la producción de información que contribuya a salvaguardar la seguridad interna y a prevenir el sabotaje, el terrorismo, el espionaje y la práctica de actos que, por su naturaleza, puedan alterar o destruir el Estado de derecho constitucionalmente establecido (art. 21 LQSIRP y art. 3.3 LOSIRP).

En lo que respecta a la actividad que llevan a cabo, aunque la producción de información no cuenta, en Portugal, con una definición legal, ha sido entendida, por quienes han escrito sobre el tema, como una actividad compleja y dinámica que busca seguir el juego de intereses entre Estados y otros actores formales e informales y determinar las amenazas al Estado de derecho democrático. Se trata de información producida en el marco de un ciclo propio, que implica un encargo para realizar una actividad; una fase de obtención de los elementos necesarios; el análisis de los mismos con el fin de elaborar una conclusión sobre el tema en cuestión; y, al final, la difusión a los responsables públicos competentes. Dado que estos elementos hacen más previsible la evolución de esas realidades, cabe señalar que constituyen un importante instrumento de ayuda a la toma de decisiones políticas de carácter estratégico y táctico[1].

Y aquí, al igual que en otros países, hay dos particularidades inherentes al funcionamiento de estos servicios que no han escapado a la atención del legislador portugués. Una es la sujeción automática al secreto de Estado de los datos y la información cuya difusión pueda causar daños a los intereses fundamentales del Estado (art. 32.1 LQSIRP). La otra es la sujeción de sus funcionarios y agentes a un deber de confidencialidad sobre las actividades de las que tengan conocimiento en razón de sus funciones y sobre la estructura y el funcionamiento de todo el sistema (art. 28)[2].

En el ordenamiento jurídico portugués, un punto de extrema importancia es la separación que existe entre la actividad de los servicios de inteligencia y la del proceso penal. Tal y como se desprende expresamente de los arts. 4.1

1. Acerca del ciclo de inteligencia, McDowell, D., *Strategic Intelligence: A Handbook for Practitioners, Managers, and Users*, The Scarecrow Press, Inc., 2009, págs. 17-24.

2. Mencionando el secreto de Estado y el deber de confidencialidad como dos características específicas de los organismos del SIRP, cf. la sentencia del Tribunal Constitucional 233/1997, punto 5. Cabe precisar que, si bien el régimen del secreto de Estado se regula, en general, en la Ley Orgánica n.º 2/2014, de 6 de agosto, y su control en la Ley Orgánica n.º 3/2014, de 6 de agosto, es, sin embargo, la LQSIRP, como ley especial sobre esta materia, la que nos interesa. Sobre el diferente ámbito de aplicación de una y otra ley a la luz del régimen anterior, Teles Pereira, T., «O segredo de Estado e a jurisprudência do Tribunal Constitucional», en Tribunal Constitucional, en *Estudos em Homenagem ao Conselheiro José Manuel Cardoso da Costa*, Coimbra Editora, Coimbra, 2003, págs. 776-777.

LQSIRP y 6.2 LOSIRP, los funcionarios y agentes de los servicios no pueden ejercer poderes, realizar actos o actividades que sean competencia específica de los tribunales o de las entidades con funciones policiales. En virtud de los apartados 2 y 3 de dichos artículos, tampoco pueden detener a personas ni instruir procesos penales[3].

La diferencia entre el ámbito de la inteligencia y el del proceso penal puede describirse, en su forma más simple, de la siguiente manera: por un lado, la investigación criminal comienza cuando el Ministerio Público tiene conocimiento del delito (art. 262.2 Código Procesal Penal de 1987), interviniendo entonces la policía criminal para investigar su existencia y autoría, es decir, en el ámbito de la represión; por otro lado, la inteligencia se sitúa antes de la existencia de la *notitia criminis*. Se trata, por tanto, de una actividad «típicamente preventiva» o administrativa[4].

Lo que equivale a afirmar que se trata de una actuación que se encuentra, por tanto, en una fase muy preliminar. Para explicar mejor sus particularidades, su objetivo es identificar amenazas contra el Estado de derecho democrático que aún no han adquirido la suficiente relevancia como para iniciar un proceso penal. No les corresponde investigar delitos concretos — tarea

3. No obstante, los funcionarios de los servicios de inteligencia, al igual que cualquier ciudadano común, pueden detener a una persona en flagrante delito si las autoridades judiciales o policiales no están presentes ni pueden ser llamadas a tiempo (art. 255.1.b) Código Procesal Penal).

4. Pereira, R. «A Produção de Informações de Segurança no Estado de Direito Democrático», in *Lusíada – Revista de Ciência e Cultura – Serie Especial – Informações e Segurança Interna*, 1998, pág. 41. Sobre el momento temporal en que se puede iniciar la investigación penal, cf. también Fernanda Palma, M., «Introdução ao Direito da Investigação Criminal e da Prova», en *Direito da Investigação Criminal e da Prova*, coordinadores Maria Fernanda Palma, Augusto Silva Dias, Paulo de Sousa Mendes, Carlota Almeida Almedina, Coimbra 2014, pág. 16. Sobre el ámbito de intervención de la policía criminal y sobre la naturaleza administrativa de la prevención, Silva Dias, A., Soares Pereira, R., *Sobre a Validade de Procedimentos Administrativos Prévios ao Inquérito e de Fases Administrativas Preliminares no Processo Penal*, Almedina, Coimbra, 2018, págs. 9-10 y pág. 12. Tradicionalmente, era posible diferenciar claramente entre represión y prevención. En el primer caso, se refería a la justicia penal, como actividad que, al estar regulada por la legislación procesal penal, se orientaba hacia el pasado mediante la respuesta a la sospecha de un delito supuestamente cometido. En el segundo caso, el de la prevención, se trataba de una actividad competencia de la Administración Pública (dirigida por el Gobierno), regulada por los respectivos ordenamientos jurídicos y reglamentarios, y orientada hacia el futuro, con el fin de prevenir un peligro concreto que «puede proyectarse en un perjuicio sobre los bienes jurídicos». Hoy en día, ya no es fácil trazar la frontera entre la prevención y la represión, dada la existencia de «investigaciones de campo avanzadas» (*Vorfeldermittlungen*), como actividad de recopilación de información que tiene lugar antes de que se produzca el peligro concreto y la sospecha del delito. Sobre esto, en Alemania, Weßlau, E., *Vorfeldermittlungen — Probleme der Legalisierung „vorbeugender Verbrechens bekämpfung« aus strafprozeßrechtlicher Sicht*, Duncker & Humblot, Berlin, 1989, pág. 26; y, en Portugal, Costa Andrade, M., *«Bruscamente no Verão Passado», A Reforma do Código de Processo Penal – Observações críticas sobre uma lei que podia e devia ter sido diferente*, Coimbra Editora, Coimbra, 2009, págs. 129-130.

que incumbe a la policía criminal —, sino producir información prospectiva[5]. Esto no quiere decir, cabe destacar, que no pueda existir, dentro de ciertos límites, una articulación entre el ámbito funcional de la producción de información y el ámbito del proceso penal u otros ámbitos estatales. De hecho, el SIED y el SIS están obligados a comunicar los hechos que puedan constituir delitos penales a las entidades competentes para la investigación criminal y el ejercicio de la acción penal, aunque, cabe señalar, con la salvaguarda de lo dispuesto en la ley en materia de secreto de Estado (art. 26.d) y art. 33.d) LOSIRP). Del mismo modo, también están obligados a comunicar las noticias e informaciones de que tengan conocimiento y que se refieran a la seguridad interna y a la seguridad del Estado, así como a la prevención y represión de la delincuencia, a las entidades que, según la ley, sean competentes (art. 26.e), y art. 33.e))[6].

A la luz de lo expuesto, parece claro que la compatibilidad de la actividad de estos organismos con la ley y con la Constitución debe ser fiscalizada de forma estricta y rigurosa. Como ya hemos visto, estos organismos no solo se ocupan de asuntos muy delicados, sino que también mantienen una estrecha relación con el primer ministro y otros miembros del Gobierno[7]. Por lo tanto, para garantizar que actúen dentro de sus funciones y no pongan en peligro los derechos de los ciudadanos, se ha creado, como principal órgano de control, el Consejo de Fiscalización del Sistema de Información de la República Portuguesa (CFSIRP), que, elegido por la Asamblea de la República (art. 8.1, de la LQSIRP), ejerce una fiscalización periódica y inspectora. Por su parte, para el control de los datos recopilados, se instituye la Comisión de Fiscalización de Datos del Sistema de Información de la República Portuguesa (CFDSIRP), que,

5. A modo de ejemplo, en lo que respecta al tráfico de drogas, la función del SIS no es investigar delitos concretos, sino producir información prospectiva sobre, por ejemplo, los países de origen, las rutas utilizadas, los mercados, el modus faciendi y las conexiones de los cárteles con la comunidad financiera. Cf. Pereira, R., «A Produção de Informações de Segurança no Estado de Direito Democrático», in *Lusíada – Revista de Ciência e Cultura –Serie Especial– Informações e Segurança Interna*, 1998, págs. 40-41.

6. Entre las competencias del CFSIRP se encuentran, por citar solo algunos ejemplos de la lista del art. 9.2 LQSIRP, la evaluación de los informes de actividades; la recepción de la lista completa de los procesos en curso; el conocimiento de los criterios de orientación gubernamental; la realización de visitas de inspección, con o sin previo aviso; la solicitud de elementos de los centros de datos; y la emisión de dictámenes. En cuanto a la CFDSIRP, que, como sugerimos en el texto, tiene un carácter más reducido en materia de fiscalización, el art. 26 solo prevé la verificación periódica de los programas, datos e información; el acceso a los mismos cuando se considere que su recopilación es ilegítima o infundada; y la posibilidad de ordenar la cancelación o rectificación de aquellos que impliquen una violación de derechos, libertades y garantías, con el correspondiente ejercicio de la acción penal, si fuera el caso. Además de estas comisiones, la Ley Orgánica n.º 4/2017 designó a una formación de las secciones penales del Tribunal Supremo de Justicia para el control judicial y la autorización previa del acceso a los datos de base y de localización de los equipos (art. 8).

7. Freitas do Amaral, D., *Curso de Direito Administrativo*, 4.ª ed., Vol. I, Almedina, Coimbra 2016, pág. 272.

a su vez, está formada por magistrados del Ministerio Público y desempeña un papel más discreto en la fiscalización del sistema, ya que sus escasas competencias solo se centran en el ámbito sensible del uso de la informática (art. 26).

Aunque la naturaleza del CFDSIRP no está del todo clara, es habitual que la doctrina administrativa incluya al CFSIRP en la categoría de «autoridades administrativas independientes». Estas últimas autoridades gozan de independencia en términos orgánicos —en lo que respecta a la composición, el modo de designación de los titulares de sus órganos, las normas relativas al mandato y el régimen de incompatibilidades— y en términos funcionales, ya que no están sujetas a órdenes o instrucciones del Gobierno ni de ninguna otra autoridad, salvo los tribunales. Sin embargo, no tienen carácter judicial o cuasi jurisdiccional, sino únicamente administrativo[8].

## 3. Los medios de obtención de información de los servicios de inteligencia portugueses: situación actual

Ahora que conocemos el marco jurídico del SIRP, el siguiente paso consiste en analizar los medios de que disponen los servicios de inteligencia portugueses para el cumplimiento de sus funciones. Para ello, hay que tener en cuenta, en primer lugar, los medios que la ley confiere expresamente al SIS y al SIED; en segundo lugar, aquellos cuyo uso ofrece margen para dudas por la ausencia de una previsión legal clara y expresa; en tercer lugar, los medios que están prohibidos por la ley o por la Constitución.

Comenzando por los medios de obtención de información expresamente previstos en la ley, el primer aspecto a destacar es que, en comparación con lo que ocurre con otros organismos europeos similares, el legislador portugués ha optado por una solución restrictiva. Como veremos más adelante, esta circunstancia ha suscitado críticas en varios sectores por la dificultad que entraña, con un marco legal tan limitado, que los servicios de inteligencia puedan llevar a cabo de manera eficaz las misiones que les incumben.

En la Sección III de la Ley 9/2007, de 19 de febrero (arts. 9 a 12) se enumeran los medios de los servicios de inteligencia. El art. 9.1 confiere a los funciona-

8. Sobre estas autoridades, como entidades asociadas al Parlamento y cuyos titulares son designados por este, con facultades de control de la legalidad administrativa y de garantía de los derechos de los ciudadanos, cf., para una breve descripción, Vieira de Andrade, J. C., *Lições de Direito Administrativo*, 5.ª ed., Imprensa da Universidade de Coimbra, Coimbra, 2017, pág. 121. Sobre las notas de independencia del CFSIRP en concreto y equiparando los cargos de presidente y miembro de dicho órgano a los de los miembros de las entidades públicas independientes previstas en la Constitución y en la ley, sentencia del Tribunal Constitucional. Y sobre la naturaleza de estas entidades en general, Canotilho, G., Moreira, V., *Constituição da República Portuguesa Anotada*, Vol. II, 4.ª ed., Coimbra Editora, Coimbra, 2014, art. 267, punto X, págs. 810-811.

rios y agentes del SIED y del SIS, siempre que estén debidamente identificados y en misión de servicio, el derecho de acceso a todas las zonas públicas, incluso aquellas de acceso restringido, y privadas de acceso público, que se consideren esenciales para el ejercicio de sus competencias. Por su parte, el art. 9.2 autoriza a los directores, directores adjuntos y directores de departamento del SIED y del SIS a acceder a la información y los registros pertinentes para el ejercicio de sus competencias, contenidos en los archivos de las entidades públicas.

También se estableció, en virtud del art. 10, la obligación de colaborar con los servicios de inteligencia a los servicios de la Administración Pública, central, regional y local, las asociaciones e institutos públicos, las empresas públicas o empresas con capital público y las concesionarias de servicios públicos (apartado 1). Esta obligación se extiende, en determinadas condiciones, a las entidades privadas que desarrollen actividades relevantes en el contexto de una relación contractual con el Estado portugués (apartado 2). Además, se impone una obligación especial de colaboración a las Fuerzas Armadas y al organismo responsable de la producción de información militar, en relación con el SIED, y a las fuerzas y servicios de seguridad, en relación con el SIS, obligándoles a facilitar, cuando se les solicite, datos y elementos relacionados con las atribuciones de los servicios de inteligencia (apartado 3 y apartado 4).

Por último, el art. 12.2 prevé la posibilidad de codificar la identidad y la categoría de los funcionarios y agentes del SIED y del SIS que desempeñan funciones en departamentos operativos, así como la expedición de documentos legales de identidad alternativa. Según el art.12.3, esta posibilidad se aplica, con las adaptaciones necesarias, a los medios materiales y equipos utilizados por los funcionarios y agentes del SIED y del SIS, en particular los vehículos de servicio operativo.

A esta lista se añadió, mediante la Ley Orgánica n.º 4/2017, de 25 de agosto, el acceso a datos de base y de localización de equipos para la producción de información necesaria para salvaguardar la defensa nacional, la seguridad interna y la prevención de actos de sabotaje, espionaje, terrorismo, proliferación de armas de destrucción masiva y delincuencia altamente organizada (art. 3).

Ante un marco legal tan reducido, surge una zona gris compuesta por medios que, en muchos casos, se utilizan sin duda en la práctica. Conviene destacar que en relación con estos medios, no existe en la legislación portuguesa una base jurídica expresa e inequívoca. De hecho, la ley ni autoriza ni prohíbe medios como, entre otros, el contacto con fuentes voluntarias de información, la observación y el seguimiento (tanto a corto como a largo plazo) y la realización de acciones encubiertas[9].

9. En el proceso penal, las acciones encubiertas están previstas en la Ley n.º 101/2001, de 25 de agosto (que establece el régimen jurídico de las acciones encubiertas con fines de prevención e investigación) y el recurso al registro de voz e imagen en el art. 6 de la Ley n.º 5/2002, de 11 de enero (que establece medidas para combatir la criminalidad organizada).

Sin embargo, está prohibido realizar interceptaciones telefónicas y acceder a datos de tráfico. Es decir, los servicios de inteligencia portugueses no pueden acceder al contenido de las comunicaciones telefónicas, ni al conjunto de información relativa al tipo, hora, duración, intensidad de uso o, en otras palabras, a las circunstancias en las que se realizan las comunicaciones[10]. Como tendremos ocasión de profundizar, en virtud del art. 34.4 CRP, estos medios solo pueden utilizarse en el marco de la fase de investigación del proceso penal[11].

En resumen, a diferencia de otros países, los servicios de inteligencia portugueses no pueden, según el marco legal, utilizar medios de inteligencia de señales (SIGINT), en particular en lo que se refiere a la inteligencia de comunicaciones (COMINT). Incluso ciertos medios de inteligencia humana (HUMINT) plantean dudas sobre su legalidad, dado el silencio de la ley portuguesa en lo que respecta, por ejemplo, al uso de acciones encubiertas. Por lo tanto, se puede concluir que la inteligencia de fuentes abiertas (OSINT), es

10. Un ejemplo es la facturación detallada, que permite conocer las condiciones reales en las que se produjo la comunicación, como todas las llamadas realizadas desde un número de teléfono por terceros, familiares u otras personas, así como sus destinatarios, números llamados, hora, duración, costes, entre otros. Cf. Pinto Monteiro, A., «A Protecção do Consumidor de Serviços Públicos Essenciais», en *Estudos de Direito do Consumidor – Centro de Direito do Consumo*, núm. 2, director Antonio Pinto Monteiro, 2000, págs. 345-346. En el ámbito del correo electrónico, tal y como se ha afirmado recientemente en la sentencia del Tribunal Constitucional 687/2021, punto 34, la visualización de un buzón de correo electrónico también permite, a su vez, conocer datos relativos al remitente y los destinatarios de los mensajes, el número de interacciones comunicativas, la fecha y la hora en que se envió un correo electrónico y el volumen de datos transmitidos. Los datos de tráfico no deben confundirse con los datos de base y los datos de localización, cuyo acceso, como hemos visto, ya está autorizado por la Ley Orgánica n.º 4/2017. En la Ley n.º 41/2004, de 28 de agosto, sobre la protección de datos personales y la privacidad en las telecomunicaciones, se menciona la categoría de datos de tráfico, definidos por dicha ley como cualquier dato tratado con fines de envío de una comunicación a través de una red de comunicaciones electrónicas o con fines de facturación de la misma (art. 2.1.d)). También se menciona la categoría de los datos de localización, como datos tratados en una red de comunicaciones electrónicas o en el marco de un servicio de comunicaciones electrónicas que indiquen la posición geográfica del equipo terminal de un usuario de un servicio de comunicaciones electrónicas accesible al público (e)). A estas dos categorías se añade, mediante la Ley n.º 32/2008, de 17 de julio, la de los datos conexos necesarios para identificar al abonado o al usuario (art. 2.1.a)). En un sentido similar, cf. el art. 2.2 de la LO n.º 4/2017, que, bajo el concepto más amplio de datos de telecomunicaciones e Internet, distingue entre datos básicos (a)), datos de localización de equipos (b)) y datos de tráfico (c)).

11. De acuerdo con el art. 187.1 Código Procesal Penal, la interceptación y grabación de conversaciones o comunicaciones telefónicas solo pueden ser autorizadas durante la fase de investigación, si existen razones para creer que la diligencia es indispensable para el descubrimiento de la verdad o que la prueba sería, de otro modo, imposible o muy difícil de obtener, mediante auto motivado del juez de instrucción y a solicitud del Ministerio Público, respecto de los delitos previstos en la norma. Este régimen se extiende, en virtud del art. 189.2, a los registros de la realización de conversaciones o comunicaciones.

decir, la recopilación y el análisis de datos e información legalmente disponibles al público, constituye una dimensión extremadamente relevante de la actividad de producción de información.

## 3.1. El problema del acceso a los datos de tráfico

El problema más debatido en Portugal en relación con el refuerzo de los métodos de los servicios de inteligencia es el acceso a los datos de tráfico. El art. 34.1 CRP proclama que «el domicilio y el secreto de la correspondencia y de los demás medios de comunicación son inviolables». En el apartado 4 se establece que «queda prohibida toda injerencia de las autoridades públicas en la correspondencia, las telecomunicaciones y los demás medios de comunicación privados, salvo en los casos previstos por la ley en materia de proceso criminal»[12].

A la luz de lo dispuesto en el art. 34.4 CRP, el problema del acceso a los datos de tráfico por parte del SIS y del SIED se ha dividido en dos cuestiones. En primer lugar, saber si los datos de tráfico están protegidos por la tutela constitucional de la inviolabilidad de las telecomunicaciones. En segundo lugar, determinar si los procedimientos de inteligencia pueden incluirse «en materia de proceso criminal», es decir, en los fines que justifican las restricciones a ese derecho.

### 3.1.1. El ámbito de protección del derecho al secreto de las telecomunicaciones

En lo que respecta al primer problema, en Portugal se ha reiterado que la inviolabilidad prescrita en el art. 34.4 CRP no se refiere únicamente a la palabra escrita y a la palabra hablada, intrínsecas a un proceso comunicativo, ni al contenido de dicho proceso comunicativo. Dado que el proveedor del servicio de telecomunicaciones ocupa una posición dominante en el proceso comunicativo, se afirma que el núcleo de esa tutela jurídica es la protección de la confianza en la seguridad y la confidencialidad de los sistemas de telecomunicaciones[13]. Y dado que esa posición dominante se ejerce tanto sobre

12. Esta última norma permanece inalterada desde la Ley Constitucional n.º 1/97, de 20 de septiembre (cuarta revisión constitucional).

13. Costa Andrade, M., *«Bruscamente no Verão Passado», A Reforma do Código de Processo Penal – Observações críticas sobre uma lei que podia e devia ter sido diferente*, Coimbra Editora, Coimbra, 2009, pág. 158. En la dogmática española, en el sentido de que lo que se protege no es únicamente el mensaje o el contenido, sino el conjunto de la comunicación, Rebollo Delgado, L., «El secreto de las comunicaciones: problemas actuales», en *Revista de Derecho Político*, núm. 48-49, 2000, pág. 365. En el sentido de que se trata del reconocimiento de un ámbito individual de inmunidad frente a posibles agresiones al proceso de comunicación en sí mismo, independientemente de cuál haya sido su contenido, Manuel

el contenido como sobre el tráfico, se concluye que la prohibición de interferir en las telecomunicaciones no se limita al conocimiento del contenido del proceso comunicativo. Esta prohibición se extiende también «durante todo el tiempo en que sea posible detener, «conservar», manipular, acceder y aprovechar su contenido o los datos externos de la comunicación». Como resultado, esa tutela abarca tanto el contenido como los datos externos de la comunicación[14].

Esta fue la interpretación defendida por el Tribunal Constitucional en sus pronunciamientos sobre la legitimidad constitucional del acceso a los datos de tráfico por parte de los organismos del SIRP. En 2015, el Tribunal Constitucional se pronunció a favor de la inconstitucionalidad de la norma del Decreto n.º 426/XII de la Asamblea de la República, que pretendía incluir en su competencia la recopilación de datos de tráfico, por violar el art. 34.4 CRP. En 2019, también se declaró inconstitucional la norma del art. 4 Ley Orgánica n.º 4/2017, que se refiere al acceso al SIS y al SIED a los datos de tráfico, por violar la misma norma de la Constitución. En la fundamentación de la primera decisión, el Tribunal mencionó que tanto las comunicaciones entre el emisor y el receptor como sus circunstancias deben mantenerse como una «comunicación cerrada». Y que, dado que la interacción entre personas a distancia debe realizarse a través de la «mediación necesaria de un tercero», se exige a ese operador y al Estado regulador que garanticen la «integridad y confidencialidad de los sistemas de comunicación». Del mismo modo, en la segunda decisión, el Tribunal también señaló que en esa tutela se protege tanto el proceso comunicativo como el contenido de la comunicación, pero solo cuando se trata de un «proceso comunicativo efectivo». Como resultado, esa tutela abarca tanto el contenido como los datos externos de la comunicación[15].

---

Cobo Del Rosal, *Tratado de Derecho Procesal Penal* Español, CESEJ, Madrid, 2008, pág. 415. Mencionando que lo que se protege es la comunicación y no el comunicado, Vicente Gimeno Sendra*, Manual de Derecho Procesal Penal*, Castillo de Luna, Ediciones Jurídicas, Madrid, 2015, pág. 408.

14. Costa Andrade, M., «A utilização e valorização do resultado de escutas telefónicas em processos disciplinares desportivos», en *Desporto & Direito – Revista Jurídica do Desporto*, VI, núm. 18, 2009. No obstante, es necesario que se trate de «datos procedentes de un proceso de comunicación en curso». El Tribunal Constitucional Federal Alemán (*Bundesverfassungsgericht* – BVerfG) ya ha justificado que, cuando las circunstancias o el contenido se almacenan en la esfera del suscriptor, este puede tomar sus propias precauciones contra el acceso secreto (decisión de 27.02.2008 - 1 BvR 370/07, 1 BvR 595/07, 185 y 190). En la jurisprudencia portuguesa, el Tribunal Constitucional ha excluido del ámbito de protección del art. 34 los datos de base relativos a la mera identificación de un usuario y los datos de localización, cuando no respaldan una comunicación concreta. No obstante, están protegidos por el art. 26.1 (sentencia 403/2015, punto 15, y sentencia 420/2017, punto 13) o, por tratarse de datos personales, por el art. 35 (sentencia 464/2019, punto 8).

15. Sentencias del Tribunal Constitucional 403/2015 y 464/2019.

## 3.2. La cuestión de la inclusión de la inteligencia en el ámbito de la «materia de proceso criminal»

Dado que los datos de tráfico están protegidos por el secreto de las telecomunicaciones, la segunda cuestión que se debatió, en el marco del problema del acceso a dichos datos por parte de los servicios de inteligencia, fue si la inteligencia puede incluirse en la expresión «materia del proceso criminal» del art. 34.4.

En esta norma, es la propia Constitución la que prevé directamente una determinada restricción, por lo que el grado de vinculación del legislador ordinario es, en consecuencia, mayor. De hecho, los propios fines de la restricción del derecho a la inviolabilidad de las telecomunicaciones se indican expresamente en dicha norma. El legislador no solo declaró que esto puede suceder «en los casos previstos por la ley», sino que, yendo más allá, tuvo el cuidado de enunciar expresamente la «materia del proceso criminal» como el ámbito en el que se pueden subsumir estos casos[16]. Por esta razón, la doctrina constitucional clasifica este precepto como de «reserva cualificada». Esto significa que el legislador ordinario solo está autorizado a restringir el contenido de este derecho para los fines allí mencionados, para la protección de los derechos o valores expresamente declarados o, en última instancia, para otros que se deriven necesariamente o que puedan considerarse implicados[17].

El Tribunal Constitucional siguió esta interpretación, afirmando que la Constitución, al particularizar el ámbito normativo de la materia penal, no limitó la injerencia al ámbito de protección de este derecho fundamental mediante la expresión «en los términos de la ley», donde se admitiría una competencia genérica de regulación. Por el contrario, mediante la formulación gramatical adoptada, autorizó la restricción de la inviolabilidad de las telecomunicaciones con la «discriminación de los fines e intereses que persigue la ley restrictiva» o «con el criterio que debe guiar la intervención del legislador ordinario»[18].

---

16. Cf. Sentencia del Tribunal Constitucional 241/2002, punto 10; Marques da Silva, G., «A utilização e valorização do resultado de escutas telefónicas em processos disciplinares desportivos» en *Desporto & Direito – Revista Jurídica do Desporto*, VI, núm.18, 2009, pág. 417.

17. Vieira de Andrade, J. C., *Os Direitos Fundamentais na Constituição Portuguesa de 1976*, 6.ª ed., Almedina, Coimbra, 2019, págs. 278-279.

18. Sentencia del Tribunal Constitucional 403/2015, punto 16. También en línea con lo expuesto en el texto, Sentencia del Tribunal Constitucional 464/2019, punto 9.2. Cabe destacar también que, según la calificación que les otorga la Constitución, el derecho al domicilio y el secreto de las comunicaciones privadas tienen carácter de «derechos inviolables», al igual que el derecho a la vida (art. 24) y el derecho a la integridad moral y física (art. 25). Lo que se pretende es limitar la posibilidad de restricciones, sometiéndolas a requisitos materiales muy vinculantes. Cf. Canotilho, G., Moreira, V., *Constituição da República Portuguesa Anotada*, Vol. I, 4.ª ed., Coimbra Editora, Coimbra, 2007, Art. 34, punto II, págs. 539-540.

Sin embargo, en las declaraciones de voto adjuntas a las dos sentencias del TC citadas es posible encontrar una línea de interpretación que, en desacuerdo abierto con la opinión mayoritaria de los jueces de dicho Tribunal, encuentra un paralelismo entre los fines perseguidos por los servicios de inteligencia y los del proceso penal. A través de esta interpretación, no encuentran ningún obstáculo para la subsunción de las actividades preventivas del SIED y del SIS en el ámbito de la restricción del art. 34.4.

Precisamente en este sentido se posicionó Maria Lúcia Amaral en su voto particular al fallo del Tribunal Constitucional 403/2015. Bajo la necesidad de la existencia de servicios de inteligencia, considera que estos se justifican por la «necesidad de salvaguardar bienes jurídicos, colectivos e individuales, que ocupan en la axiología constitucional un lugar no menor que los bienes protegidos por normas penales incriminatorias». Así, defendió una «afinidad valorativa o teleológica entre los fines perseguidos por los servicios de inteligencia y las normas penales incriminatorias»[19].

Cabe señalar que este argumento no puede ser válido. Por un lado, no se niega que estos servicios se basan en la Constitución, ya que, además de tener su fundamento constitucional expreso en el art. 164.q) el Estado tiene no solo la obligación evidente de abstenerse e interferir en los derechos fundamentales, sino también la tarea positiva de garantizarlos y hacer que todos los respeten[20]. Asimismo, se acepta, en cualquier caso, que no solo es posible que la actividad de inteligencia sea materialmente investigadora, sino que también existen fenómenos, sobre todo en materia de delincuencia más compleja, que pueden merecer una atención paralela por parte de los servicios de inteligencia y los órganos de policía criminal. Pero si estos son dos puntos que nos parecen inequívocos, otro completamente distinto —y con el que no estamos de acuerdo— es partir de las importantes misiones de salvaguarda de los bienes jurídicos esenciales para la subsistencia del Estado de derecho democrático que evidentemente cumplen y, a partir de ahí, establecer una afinidad entre ellas y las del proceso penal.

19. Punto 4 de su declaración de voto.

20. Canotilho, G., Moreira, V., *Constituição da República Portuguesa Anotada*, Vol. I, 4.ª ed., Coimbra Editora, Coimbra, 2007, art. 9, punto IV, pág. 277. Es cierto que, debido a las particularidades de su actividad, la base constitucional de los servicios de inteligencia no está totalmente exenta de dudas. En otros contextos jurídicos, este es un tema tradicionalmente problemático. En la doctrina española, en el sentido de que «el mundo de los servicios de Inteligencia resulta, todavía hoy, por completo opaco a las Constituciones escritas. Revenga Sánchez, M., «Servicios de inteligencia y derecho a la intimidad», en *Revista Española de Derecho Constitucional*, 21, núm. 61, 2001, pág. 61. En Portugal, la garantía de la seguridad se basa en las tareas impuestas al Estado de garantizar la independencia nacional y crear las condiciones políticas, económicas, sociales y culturales que la promuevan, así como garantizar los derechos y libertades fundamentales y el respeto de los principios del Estado democrático de derecho (art. 9a) y b)); así como en el art. 27 y en los arts. 272 y 273 de la CRP, tal y como se señala en la sentencia del Tribunal Constitucional 464/2019, punto 7.

Es importante tener en cuenta que los servicios de inteligencia no son órganos de la policía criminal. Como hemos visto, por imposición de la ley, no pueden ejercer poderes, realizar actos que sean competencia de las entidades policiales ni instruir procesos penales. Mientras que la actividad del Ministerio Público se rige por el principio de legalidad, con la obligación de abrir una investigación tan pronto como se tiene conocimiento del delito, la producción de información se lleva a cabo por razones de oportunidad y conveniencia. Si en un caso existe una investigación dirigida por el Ministerio Público y una relación de dependencia funcional entre los órganos de policía criminal y las autoridades judiciales, en el otro se trata de una actividad dirigida por entidades administrativas, sin más que un control de carácter administrativo. Y si, por un lado, hay una acción mayoritariamente abierta y pública, por otro lado, hay una actuación sujeta al secreto de Estado[21].

En resumen, como hemos visto, la Constitución fue clara y expresa al prever la restricción del derecho al secreto de las telecomunicaciones solo para los casos relacionados con procesos penales. Además, teniendo en cuenta lo expuesto anteriormente, no es posible incluir la actividad de inteligencia en el ámbito del proceso penal. Por lo tanto, se puede estar de acuerdo con la sentencia 464/2019 del Tribunal Constitucional cuando afirma que el art. 34.4 consagra una «reserva absoluta de proceso criminal».

Llegados a este punto, sabemos ahora, por un lado, que los datos de tráfico, con la noción que se ha expuesto, al estar protegidos por la inviolabilidad de las telecomunicaciones, están incluidos en el ámbito de protección del art. 34.4. Por otro lado, también sabemos que la inteligencia no se subsume en los fines expresamente admitidos para la restricción de ese derecho fundamental. Una vez respondidos los dos problemas fundamentales que se plantearon al principio de este punto, solo cabe dar una respuesta a la cuestión central que se formuló: que el acceso a los datos de tráfico por parte de los servicios de inteligencia aún no es constitucionalmente conforme con el parámetro del secreto de la correspondencia y de los demás medios de comunicación privada. Por lo tanto, la solución obvia para superar la garantía absoluta que allí se establece será mediante una revisión constitucional[22].

## 4. Perspectivas futuras

A pesar de la restricción impuesta por el art. 34.4 CRP, hoy en día varios sectores de la sociedad portuguesa exigen que, en el futuro, se revise esta norma, de modo que los servicios de inteligencia puedan acceder y analizar los datos de tráfico.

21. Sobre las diferencias entre la inteligencia y el proceso penal, *supra*, 2.

22. Es lo que también afirma Vieira de Andrade, J. C., *Lições de Direito Administrativo*, 5.ª ed., Imprensa da Universidade de Coimbra, Coimbra, 2017, págs. 84-85.

Se reconoce la naturaleza esencialmente reactiva y no preventiva del derecho penal y el hecho de que este opera dentro de un proceso penal que solo tiene su inicio con la adquisición de la noticia del delito. Por lo tanto, este no conserva utilidades (por el contrario, presenta limitaciones) desde la perspectiva de intervenir legítima y eficazmente en el control de fenómenos como la amenaza terrorista. Y así, se plantea la cuestión de cómo llevar a cabo, en el seno de Estados democráticos basados en un derecho penal del hecho y no en el derecho penal del agente, una lucha preventiva contra el delito, es decir, antes de que este se produzca[23].

Y es, sobre todo, la importancia que la información revelada por los datos de tráfico tiene a efectos de prevención del terrorismo lo que ha estado subyacente a las propuestas presentadas para incluir su obtención en la lista de medios de actuación del SIRP. De hecho, dado que la amenaza terrorista contemporánea se desarrolla en redes (mediante conexiones entre personas situadas en puntos geográficos distantes), los elementos informativos que proporcionan esos datos son relevantes para la prevención del terrorismo. A través de este acceso es posible, por ejemplo, extraer inferencias relevantes sobre, por ejemplo, el conjunto de individuos contactados por sospechosos de estar involucrados en actividades terroristas, la indicación de los lugares que frecuentan, etc. Lo que permite, a su vez, establecer importantes conexiones entre personas y lugares que los servicios hipotéticamente necesitan a efectos de análisis[24].

Además, teniendo en cuenta que la prevención del terrorismo exige un intercambio eficaz de información entre los servicios portugueses y sus homólogos, cabe señalar que el acceso al tráfico de comunicaciones puede ser un medio privilegiado para materializar esa cooperación. De hecho, como se ha destacado insistentemente, Portugal es, en realidad, el único país de la Unión Europea cuyo ordenamiento jurídico no autoriza en este ámbito métodos de vigilancia de las telecomunicaciones. Por esta razón, se manifiesta preocupación por el hecho de que los servicios de inteligencia portugueses se encuentren en una situación de clara desventaja con respecto a sus homólogos[25].

---

23. Manuel Abrantes, A. M. «Limites Constitucionais à (Excessiva) Antecipação da Tutela Penal nos Crimes de Terrorismo – Anotação às decisões n.ºs 2016-611 QPC e 2017-625 QPC do Conselho Constitucional francês», en *Revista Portuguesa de Ciência Criminal*, 27, núm. 2, 2017, pág. 435.

24. En este sentido, cf. la declaración de voto de Teles Pereira a la sentencia del Tribunal Constitucional 403/2015, punto 11.2.

25. Pereira, R., «Informações e Investigação Criminal», en *I Colóquio de Segurança Interna*, coordinador Manuel Monteiro Guedes Valente, Almedina, Coimbra, 2005, pág. 162. Hecho que se confirma en el informe «Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU» da European Union Agency for Fundamental Rights (FRA). Cf. el volumen I: Member States' legal frameworks, 2015, pág. 20, y el volumen II: field perspectives and legal update, 2017, pág. 40.

Ante esto, no es difícil concluir que, recordando las misiones reconocidas a los servicios de inteligencia, la recopilación de datos externos de las comunicaciones, al ser plenamente adecuada para el ejercicio de las funciones del SIED y del SIS, constituiría obviamente un instrumento de gran importancia para la producción de la información necesaria para la preservación de la seguridad interna y externa. Por lo tanto, una revisión del texto de la Constitución que dejara de impedirlo permitiría, sin duda, garantizar la seguridad a otros niveles.

Y lo cierto es que hay países de otros ámbitos jurídicos europeos, con un horizonte jurídico bastante similar al portugués, cuyas constituciones, debido a la configuración de las restricciones a la privacidad de las comunicaciones, ya están preparadas para que las agencias de inteligencia procedan a interceptar las telecomunicaciones. En Alemania, el art. 10.2 *Grundgesetz* tolera las excepciones al derecho a la privacidad de la correspondencia, las comunicaciones postales y las telecomunicaciones mediante la frase «de conformidad con la ley» y, yendo más allá, establece además que si la restricción sirve para la protección del orden democrático o la seguridad federal o estatal, la ley puede prever que no se informe a la persona afectada de la restricción y que el recurso ante los tribunales sea sustituido por un control efectuado por organismos designados por el poder legislativo. El art. 15 de la Constitución de la República Italiana presenta un grado idéntico de flexibilidad al autorizar las limitaciones a la libertad y el secreto de la correspondencia y otras formas de comunicación mediante «acto motivado de la autoridad judicial con las garantías establecidas en la ley». Por último, cabe mencionar que la Constitución Española, en el art. 18.3, permite, de forma aún más simple, las restricciones al secreto en las telecomunicaciones mediante la expresión genérica «resolución judicial»[26].

26. La problemática en juego no es nueva, ya que antes de la Ley Constitucional n.º 1/2001 ya se había recomendado una modificación para que se añadiera al artículo actual, en materia de restricciones, la «prevención del espionaje y de la delincuencia violenta o altamente organizada, incluidos el terrorismo y el tráfico de personas, armas y estupefacientes, previa autorización judicial». Cf. Pereira, R. «Os desafios do terrorismo: a resposta penal e o sistema de informações», en *Informações e Segurança – Estudos em Honra do General Pedro Cardoso*, coordinador Adriano Moreira, Prefácio, Lisboa, 2004, pág. 527, nota 45. En el sentido de que, en lo que respecta al ordenamiento jurídico italiano y alemán, la consagración legal de restricciones se enfrenta a menos dificultades en comparación con el portugués, teniendo en cuenta las fórmulas amplias y genéricas que han sido adoptadas por dichos instrumentos normativos, cf. la sentencia del Tribunal Constitucional 198/85, punto 2. El caso portugués no es único en el mundo, ya que la Constitución de la República Federativa de Brasil optó por una fórmula similar a la portuguesa al establecer en el art. 5, XII, que «es inviolable el secreto de la correspondencia y de las comunicaciones telegráficas, de datos y telefónicas, salvo, en este último caso, por orden judicial, en los supuestos y en la forma que la ley establezca a efectos de investigación criminal o instrucción procesal penal». Y también en Brasil se ha prohibido a los órganos que componen el Sistema Brasileño de Inteligencia (SISBIN) el envío de datos a la Agencia Brasileña de Inteligencia (ABIN) que impliquen la violación del secreto telefónico o de datos, dado que esta es una competencia conferida al Poder Judicial, en los términos previstos constitucionalmente. Cf. el voto de la ministra Cármen Lúcia en ADI 6529 MC / DF, de 13/08/2020.

En este sentido, teniendo en cuenta que los obstáculos planteados en esa línea jurisprudencial solo pueden superarse mediante una revisión del texto de la Constitución, el *Partido Social Democrata* (PSD) presentó el Proyecto de Revisión Constitucional núm. 7/XV/1.ª. A la configuración actual de la norma del art. 34, pretendía añadir un nuevo apartado, el n.º 5, que establecería que «La ley puede autorizar el acceso del sistema de información de la República a los datos de contexto resultantes de las telecomunicaciones, sujeto a decisión y control judiciales». A este debate se sumó el *Partido Socialista* (PS), que, en el Proyecto de Revisión Constitucional núm. 3/XV, pretendía añadir un apartado 6. Esta norma establecería que «se excluye de lo dispuesto en el apartado anterior el acceso, mediante autorización judicial, por parte de los servicios de información, a los datos básicos, de tráfico y de localización de equipos, así como a su conservación, con el fin de producir la información necesaria para salvaguardar la defensa nacional, la seguridad interna y la prevención de actos de sabotaje, espionaje, terrorismo, proliferación de armas de destrucción masiva y delincuencia altamente organizada, en los términos que se definan por ley». Sin embargo, este proceso de revisión constitucional no obtuvo resultados[27].

## 5. Conclusiones

Desde un punto de vista legal, los servicios de inteligencia portugueses disponen de pocas capacidades operativas. Esta circunstancia ha llevado a que, en los últimos años, se haya debatido el refuerzo de sus medios de recopilación de información con la posibilidad de realizar escuchas telefónicas y acceder a datos de tráfico. Con todo, tal y como ha defendido la jurisprudencia constitucional portuguesa, estos medios constituyen una violación del derecho al secreto de las telecomunicaciones, previsto constitucionalmente en el art. 34.4. Esta norma solo permite restricciones a este derecho en el ámbito del proceso penal, no siendo posible establecer una equiparación entre el proceso penal y la actividad de producción de información. En lo que respecta, en particular, a los datos de tráfico —cuya información es muy útil, por ejemplo, para la prevención del terrorismo—, se reconoce que su acceso para fines de inteligencia solo será constitucionalmente legítimo con una revisión constitucional.

Por último, si en el futuro se concede al SIED y al SIS acceso a datos de tráfico y otros medios de recopilación de información, cabe esperar que los métodos que hasta ahora son excepcionales no se utilicen de forma generalizada y desmesurada. De hecho, no podemos olvidar que los métodos de recopilación de información son, sin duda, uno de los ámbitos más delicados

27. Para un análisis de estos proyectos, Narciso, J., «Serviços de Informações, Dados de Tráfego e Revisão Constitucional – Uma Análise Crítica dos Projetos de Revisão Constitucional n.º 7/XV/1.ª e n.º 3/XV», *Revista Portuguesa de Direito Constitucional*, 3, 2023.

de la inteligencia y, al mismo tiempo, uno de los ámbitos en los que es más difícil establecer un equilibrio entre la garantía de la seguridad y la protección de los derechos fundamentales[28].

## BIBLIOGRAFÍA

**Cobo del Rosal, M.**, *Tratado de Derecho Procesal Penal* Español, CESEJ, Madrid, 2008.

**Costa Andrade, M.**, «A utilização e valorização do resultado de escutas telefónicas em processos disciplinares desportivos», en *Desporto & Direito — Revista Jurídica do Desporto*, VI, núm. 18, 2009.

**Costa Andrade, M.**, *Bruscamente no Verão Passado», A Reforma do Código de Processo Penal — Observações críticas sobre uma lei que podia e devia ter sido diferente*, Coimbra Editora, Coimbra, 2009.

**Canotilho, G., Moreira, V.**, *Constituição da República Portuguesa Anotada*, Vol. I, 4.ª ed., Coimbra Editora, Coimbra, 2007.

**Canotilho, G., Moreira, V.**, *Constituição da República Portuguesa Anotada*, Vol. II, 4.ª ed., Coimbra Editora, Coimbra, 2014.

**Freitas do Amaral, D.**, *Curso de Direito Administrativo*, 4.ª ed., Vol. I, Almedina, Coimbra 2016.

**Fernanda Palma, M.**, «Introdução ao Direito da Investigação Criminal e da Prova», en *Direito da Investigação Criminal e da Prova*, coordenadores Maria Fernanda Palma / Augusto Silva Dias / Paulo de Sousa Mendes / Carlota Almeida Almedina, Coimbra 2014.

**Gimeno Sendra, G.**, *Manual de Derecho Procesal Penal*, Castillo de Luna, Ediciones Jurídicas, Madrid, 2015.

**Manuel Abrantes, A.**, «Limites Constitucionais à (Excessiva) Antecipação da Tutela Penal nos Crimes de Terrorismo — Anotação às decisões n.ºs 2016-611 QPC e 2017-625 QPC do Conselho Constitucional francês», en *Revista Portuguesa de Ciência Criminal*, 27, núm. 2, 2017.

**Marques da Silva, G.**, «A utilização e valorização do resultado de escutas telefónicas em processos disciplinares desportivos» en *Desporto & Direito — Revista Jurídica do Desporto*, VI, núm.18, 2009.

**McDowell, D.**, *Strategic Intelligence: A Handbook for Practitioners, Managers, and Users*, The Scarecrow Press, Inc., 2009.

28. Para obtener una visión detallada de las dificultades para autorizar el acceso a los datos de tráfico por parte del SIRP, João Narciso, *O Acesso a Dados de Tráfego pelo Sistema de Informações da República Portuguesa*, Gestlegal, Coimbra, 2022, págs. 87 y siguientes.

**Narciso, J.**, «Serviços de Informações, Dados de Tráfego e Revisão Constitucional — Uma Análise Crítica dos Projetos de Revisão Constitucional n.º 7/XV/1.ª e n.º 3/XV», *Revista Portuguesa de Direito Constitucional*, 3, 2023.

**Narciso, J.**, *O Acesso a Dados de Tráfego pelo Sistema de Informações da República Portuguesa*, Gestlegal, Coimbra, 2022.

**Pinto Monteiro, A.**, «A Protecção do Consumidor de Serviços Públicos Essenciais», en *Estudos de Direito do Consumidor — Centro de Direito do Consumo*, núm. 2, director António Pinto Monteiro, 2000.

**Pereira, R.**, «A Produção de Informações de Segurança no Estado de Direito Democrático», in *Lusíada — Revista de Ciência e Cultura — Serie Especial — Informações e Segurança Interna*, 1998.

**Pereira, R.**, «Informações e Investigação Criminal», en *I Colóquio de Segurança Interna*, coordinador Manuel Monteiro Guedes Valente, Almedina, Coimbra, 2005.

**Pereira, R.**, «Os desafios do terrorismo: a resposta penal e o sistema de informações», en *Informações e Segurança — Estudos em Honra do General Pedro Cardoso*, coordinador Adriano Moreira, Prefácio, Lisboa, 2004.

**Rebollo Delgado, L.**, «El secreto de las comunicaciones: problemas actuales», en *Revista de Derecho Político*, núms. 48-49, 2000.

**Revenga Sánchez, M.**, «Servicios de inteligencia y derecho a la intimidad», en *Revista Española de Derecho Constitucional*, 21, Núm. 61, 2001.

**Reis Novais, J.**, «Direitos Fundamentais e inconstitucionalidade em situação de crise — a propósito da epidemia COVID-19», en *e-Pública*, Vol. 7, núm. 1, 2020.

**Silva Dias, A., Soares Pereira, R.**, *Sobre a Validade de Procedimentos Administrativos Prévios ao Inquérito e de Fases Administrativas Preliminares no Processo Penal*, Almedina, Coimbra, 2018.

**Teles Pereira, J.**, «O segredo de Estado e a jurisprudência do Tribunal Constitucional», en Tribunal Constitucional, en *Estudos em Homenagem ao Conselheiro José Manuel Cardoso da Costa*, Coimbra Editora, Coimbra, 2003.

**Vieira de Andrade, J. C.**, *Lições de Direito Administrativo*, 5.ª ed., Imprensa da Universidade de Coimbra, Coimbra, 2017.

**Vieira de Andrade, J. C.**, *Os Direitos Fundamentais na Constituição Portuguesa de 1976*, 6.ª ed., Almedina, Coimbra, 2019.

**Wesslau, E.**, *Vorfeldermittlungen — Probleme der Legalisierung „vorbeugender Verbrechens bekämpfung« aus strafprozeßrechtlicher Sicht*, Duncker & Humblot, Berlin, 1989.

# EL SISTEMA ESPAÑOL DE INTELIGENCIA FINANCIERA PARA COMBATIR EL BLANQUEO DE CAPITALES

**Yago González Quinzán**
*Profesor e investigador predoctoral (FPU)*
*Universidad de Santiago de Compostela*

## 1. Introducción

Los Servicios de Inteligencia se concretan en España en la estructura del Centro Nacional de Inteligencia (CNI). A este organismo se le atribuye la función de informar al gobierno de amenazas contra la integridad territorial del estado, la estabilidad de las instituciones políticas o los intereses nacionales[1]. A las actividades del CNI se añade una comunidad de inteligencia conformada por organismos dedicados a campos de actuación específicos[2]. Tal es el caso del Servicio Ejecutivo de la Comisión de Prevención del Blanqueo de Capitales e Infracciones Monetarias (SEPBLAC), que se configura a nivel nacional como la Unidad de Inteligencia Financiera (UIF) contra la delincuencia económica[3].

La inteligencia financiera resulta una herramienta esencial para luchar contra delitos de dimensión transnacional y de especial gravedad para el sector económico y financiero. A través de las UIF, consideradas desde las mismas instancias supranacionales como el centro de las políticas preventivas contra el blanqueo de capitales y la financiación del terrorismo, se trata de desmantelar las redes criminales que utilizan sofisticados recursos para la perpetración de sus actividades delictivas. El objetivo es combatir el problema que representa el secreto bancario para la ocultación de beneficios ilícitos y la elusión de controles, por lo que a través del intercambio de infor-

1. Véase artículo 1 de la Ley 11/2002, de 6 de mayo.

2. Rodríguez Marcos, A. M., «Capítulo II. Seguridad e inteligencia», en López Muñoz, J. (coord.): *Manual de Inteligencia. 2ª edición*. Tirant lo Blanch, Valencia, 2023, pág. 46.

3. Llavador Piqueras, J., Llavador Cisternes, H., *El régimen jurídico de los servicios de inteligencia en España*. Tirant lo Blanch, Valencia, 2015, pág. 38.

mación financiera se logra un mecanismo clave de reacción contra la delincuencia organizada[4].

Las UIF desarrollan un papel esencial al configurarse como las agencias encargadas de la recepción y el análisis de los informes sobre operaciones sospechosas de blanqueo de capitales, delitos antecedentes y financiación del terrorismo. Resulta necesario pues dotar de las herramientas suficientes a las UIF para recabar datos de los sujetos obligados y colaborar con las autoridades administrativas y judiciales. En la actualidad, las UIF manejan un volumen de datos excesivamente amplio derivado de los informes recibidos. Por este motivo, los sistemas de inteligencia financiera deben desarrollarse más para hacer frente a una recepción y análisis de datos masiva con el fin de detectar activos ilícitos ocultados tras múltiples transferencias y cuentas bancarias[5].

La legislación de prevención de blanqueo de capitales, así como la regulación penal, ha estado sometida a una tendencia expansionista que se reclama desde la normativa internacional, especialmente por el Grupo de Acción Financiera Internacional (GAFI) y las directivas comunitarias. Lo anterior se traduce en el establecimiento en nuestro país de un sistema complejo de autoridades para la prevención (la Vigilancia Aduanera, la Agencia Tributaria, el CNI y la Comisión de Prevención del Blanqueo de Capitales e Infracciones Monetarias) y la persecución (Policía Nacional y Guardia Civil) del blanqueo de capitales y la financiación del terrorismo[6].

El origen de la Comisión de Prevención del Blanqueo de Capitales e Infracciones Monetarias se sitúa en la Ley 19/1993, de 29 de diciembre, que creó dicha entidad para el control de la supervisión de las entidades financieras. Actualmente se trata de un organismo autónomo incardinado bajo la Secretaría de Estado de Economía y Apoyo de la Empresa, dependiente a su vez del Ministerio de Economía, Comercio y Empresa[7]. La Comisión, conforme a lo contemplado en la Ley 10/2010, de 28 de abril, puede ejercer su actividad a través del Pleno o el Comité Permanente, así como mediante el Comité de Inteligencia Financiera. Como órganos de apoyo de la Comisión se establecen legalmente la Secretaría y el SEPBLAC.

El SEPBLAC actúa con plena independencia respecto a la Comisión. Es la UIF a nivel nacional[8] y le corresponde el análisis de los reportes enviados por

4. Hava García, E., «Blanqueo de capitales», en Díaz Fernández, A. M. (dir.): *Conceptos fundamentales de inteligencia*. Tirant lo Blanch, Valencia, 2016, pág. 34.

5. *Ibid.*, pág. 35.

6. Carlos de Oliveira, A. C., «The Anti-Money Laundering Architecture of Spain», en Vogel B. y Maillart, J. (eds.): *National and International Anti-Money Laundering Law*. Intersentia, Cambridge, 2020, pág. 399.

7. *Ibidem*.

8. Véase artículo 67.1 del Real Decreto 304/2014, de 5 de mayo.

los sujetos obligados en punto a crear información financiera que, si procede, remite luego al Ministerio Fiscal, a las Fuerzas y Cuerpos de Seguridad del Estado, a las autoridades judiciales o administrativas, a otras UIF extranjeras o a las autoridades europeas. También ejerce la supervisión y la ejecución de las sanciones y contramedidas estipuladas en el artículo 42 de la Ley 10/2010, de 28 de abril. Tras la reorganización de los mecanismos de supervisión, recoge la función de control de movimientos de capitales y divisas atribuidas a la Comisión de Vigilancia de las Infracciones de Control de Cambios.

Asimismo, sin perjuicio del apoyo del Banco de España, de la Comisión Nacional del Mercado de Valores (CNMV) y de la Dirección General de Seguros y de Fondos de Pensiones (DGSFP), el SEPBLAC desarrolla una función de supervisión sobre el cumplimiento por los sujetos obligados de las medidas preventivas recogidas en la Ley 10/2010, de 28 de abril. Los resultados de las actuaciones, recogidos en un informe de inspección, se remiten a la Secretaría de la Comisión, que las eleva a la consideración del Comité Permanente. También el SEPBLAC puede proponer al Comité Permanente la adopción de requerimientos instando a los sujetos obligados a adoptar las medidas correctoras que se estimen necesarias.

## 2. La inteligencia financiera en el marco de la inteligencia económica: estado de la disciplina en España

Antes de entrar a precisar qué se entiende por inteligencia económica y financiera, conviene poner de manifiesto una somera aproximación al concepto de «inteligencia». Esta categoría se identifica ampliamente como el resultado final de una serie de procesos sistemáticos de obtención de información, revisión y extracción de datos y conclusiones para una toma de decisiones correcta. Apunta Rodríguez Marcos[9] que con el término inteligencia se hace alusión a tres realidades diferentes. En primer lugar, los servicios de inteligencia como instituciones nacionales. En segundo lugar, el ciclo de inteligencia como proceso de obtención y análisis de información. Y, en tercer lugar, el producto derivado de la revisión de la información.

La inteligencia económica constituye una disciplina esencial en la política económica global y la seguridad nacional. Ampliamente se reclama su concreción en un cuerpo normativo que permita hacer frente a una «guerra de cuarta generación», que se lleva a cabo a través de ataques financieros y la vulneración de los derechos socioeconómicos de los ciudadanos. Resulta necesario, siguiendo a González Cussac[10], voz autorizada en las relaciones entre el derecho y la inteligencia, traducir el nuevo desarrollo de la inteligen-

9. Rodríguez Marcos, A. M., *op. cit.*, pág. 44.

10. González Cussac, J. L., «Inteligencia y Derecho», en Antón Mellón, J. (coord.): *Teoría de la Inteligencia en sistemas políticos democráticos*. Tirant lo Blanch, Valencia, 2024, pág. 221.

cia económica en un régimen legal que garantice la vigilancia estratégica en la toma de decisiones, la competitividad de las estructuras empresariales y la estabilidad de las economías nacionales.

En la línea de lo expuesto, la inteligencia económica se ha integrado en el concepto amplio de «seguridad» que predomina en la actualidad. La relación entre inteligencia económica y seguridad ha dado lugar a la adopción por cada país de un concreto esquema orgánico de inteligencia que puede formar parte de los propios servicios de inteligencia o, más ampliamente, de la comunidad de inteligencia, pero, en todo caso, con una coordinación efectiva entre tales servicios, gobiernos y empresas. El elemento común de todos los sistemas de inteligencia económica se vincula con la obtención, el procesamiento y la comunicación de datos financieros, económicos y empresariales para salvaguardar los intereses interiores y exteriores de un estado[11].

Para Jiménez Villalonga[12], la inteligencia económica consiste en la obtención de información financiera, económica y empresarial por un estado para preservar sus intereses económicos. Este concepto se complementa con instrucciones a las empresas sobre medidas preventivas contra espionajes económicos, inversiones de riesgo y promoción de la industria nacional. El autor centra como bases de la inteligencia económica la promoción de un entorno competitivo desde una perspectiva económica y en base a fuentes abiertas. No obstante, la evolución actual de la inteligencia económica permite extender el concepto a aquella obtenida a partir de información financiera y que realizan los órganos de la administración y los servicios de inteligencia.

En España existe una evolución notable de la inteligencia económica, sobre todo a raíz de la crisis financiera de hace algo más de una década[13]. En este sentido, se han creado diversas agencias de inteligencia para la prevención de delitos económicos y financieros. El mayor ejemplo es el SEPBLAC, a quien se atribuye la condición de UIF para la recepción, el análisis y la remisión de información financiera sobre actos de blanqueo de capitales. A lo anterior se une la creación de equipos económicos en el seno del CNI. Ello reafirma un avance de la inteligencia económica y financiera en nuestro país, mediante un sistema que relaciona entidades propias de la comunidad de inteligencia con otros órganos incluidos en el servicio de inteligencia nacional.

La inteligencia económica se destina a la protección de la seguridad nacional, que se trata en la actualidad de un concepto amplio. En aquella se integra la inteligencia financiera, que se configura como una rama concreta que trata de prevenir delitos de tipo económico o financiero, entre los que se

11. González Cussac, J. L., Larriba Hinojar, B., *Inteligencia económica y competitiva. Estrategias legales en las nuevas agendas de seguridad nacional*. Tirant lo Blanch, Valencia, 2012, pág. 40.

12. Jiménez Villalonga, R., «Capítulo IV. Tipos de inteligencia», en López Muñoz, J. (coord.): *Manual de Inteligencia. 2ª edición*. Tirant lo Blanch, Valencia, 2023, pág. 126.

13. González Cussac, J. L., Larriba Hinojar, B., *op. cit.,* pág. 44.

halla el blanqueo de capitales. La inteligencia financiera se apoya en el estudio de los movimientos financieros y el alcance de posibles redes ilícitas de financiación. La inteligencia económica, como concepto más amplio, abarca aspectos como riesgos financieros, competencia, geoeconomía y estabilidad macroeconómica. La interrelación entre la inteligencia económica y financiera se aprecia en la colaboración del SEPBLAC con los equipos del CNI.

## 3. La Comisión de Prevención del Blanqueo de Capitales e Infracciones Monetarias

La Ley 10/2010, de 28 de abril, establece como primer órgano de control para la prevención del blanqueo de capitales y la financiación del terrorismo a la Comisión de Prevención del Blanqueo de Capitales e Infracciones Monetarias. Esta entidad, incardinada en el organigrama de la Secretaría de Estado de Economía y Apoyo de la Empresa, se encarga de la promoción de la aplicación de la legislación para la prevención del blanqueo de capitales y la financiación del terrorismo[14]. Es el organismo al que le corresponde el diseño de las políticas nacionales en materia de prevención del blanqueo de capitales y la financiación del terrorismo[15] que, en todo caso, deben ser objeto de actualización periódica de conformidad con los riesgos detectados[16].

El origen de la Comisión se remonta a la Ley 19/1993, de 28 de diciembre. Esta norma, de apresurada aprobación por motivos de eficacia, supuso la creación de una estructura que recogía las competencias de la Comisión de Vigilancia de las Infracciones de Control de Cambios[17]. La puesta en marcha de la Comisión debía haberse hecho en un plazo de seis meses, en virtud de la Disposición Final Primera de la Ley 19/1993, de 28 de diciembre; sin embargo, se retrasó su inicio hasta dos años cuando, en virtud del Real Decreto 925/1995, de 9 de junio, por el que se aprobó el Reglamento de la Ley 19/1993, de 28 de diciembre, se derogó el Real Decreto 2391/1980, de 10 de octubre, regulador de la Comisión de Vigilancia de las Infracciones de Control de Cambios.

La presidencia de la Comisión de Prevención del Blanqueo de Capitales e Infracciones Monetarias corresponde al secretario de Estado de Economía y Apoyo a la Empresa. En las reuniones plenarias, el presidente convoca y dirige las deliberaciones. En la jerarquía inferior se articula toda una variada

14. Úbeda Martínez-Valera, P., *Obligaciones derivadas de la Ley de prevención del blanqueo de capitales en el ámbito de las profesiones jurídicas. Especial referencia al abogado*. Bosch, J. M., Barcelona, 2024, pág. 297.

15. Véase artículo 44.1 de la Ley 10/2010, de 28 de abril.

16. Véase artículo 62 del Real Decreto 304/2014, de 5 de mayo.

17. Alcaraz Lamana, C., *La investigación de los delitos económicos y relacionados con la corrupción. Apuntes*. Tirant lo Blanch, Valencia, 2016, pág. 30.

composición, objeto de determinación reglamentaria, en la que, en todo caso, se agrupan representantes del Ministerio Fiscal (Audiencia Nacional, Anticorrupción, Antidroga), de los ministerios con competencias en la materia, así como las autoridades autonómicas con competencia para la protección de personas y bienes y para el mantenimiento de la seguridad ciudadana[18].

La forma de actuación de la Comisión de Prevención del Blanqueo de Capitales e Infracciones Monetarias puede ser mediante el Pleno o el Comité Permanente. La asistencia es personal e indelegable[19]. Reglamentariamente también se prevé otra forma de actuación a través del Comité de Inteligencia Financiera. Tanto el Pleno como sus Comités se constituyen de forma válida en primera convocatoria con la presencia del presidente, el secretario y de la mitad al menos, de sus miembros; y, en segunda convocatoria, con la presencia de un tercio de sus miembros, incluidos presidente y secretario. La Comisión y sus Comités se reúnen con carácter general dos veces al año, sin perjuicio de reuniones adicionales cuando sean procedentes[20].

## 3.1. El Pleno de la Comisión

La primera forma en la que la Comisión puede llevar a cabo sus actuaciones es mediante el Pleno. En este último se integran representantes de toda una serie de órganos policiales, financieros y políticos que conforman una concentración de conocimiento para la adopción de las medidas de prevención. En el Pleno se agrupa el secretario de Estado de Economía y Apoyo a la Empresa, al que le corresponde la presidencia, el fiscal jefe de la Fiscalía Antidroga, el fiscal de sala jefe de la Audiencia Nacional, el secretario general del Banco de España, el director general del Registro y el Notariado, el secretario de Estado de Seguridad, el director de Inteligencia del CNI y el director del SEPBLAC, entre otros representantes.

El Pleno es el órgano superior y colegiado de la Comisión de Prevención del Blanqueo de Capitales e Infracciones Monetarias. Se trata de la principal instancia para el impulso de las actividades de prevención del blanqueo de capitales, financiación del terrorismo e infracciones de la normativa sobre transacciones económicas con el exterior. A esta función principal se añaden otras atribuciones complementarias: la aprobación de criterios para la colaboración y la coordinación de las actuaciones con otros órganos u autoridades, como las Fuerzas y Cuerpos de Seguridad del Estado, los órganos judiciales y el Ministerio Fiscal; así como la aprobación, previa consulta con el Banco de España, del presupuesto del SEPBLAC[21].

18. Véase artículo 44.3 de la Ley 10/2010, de 28 de abril.

19. Véase artículo 44.3 segundo párrafo de la Ley 10/2010, de 28 de abril.

20. Véase artículo 62.3 del Real Decreto 304/2014, de 5 de mayo.

21. Véase artículo 44.2 de la Ley 10/2010, de 28 de abril.

Una mención particular merece la elaboración de estadísticas sobre blanqueo de capitales y financiación del terrorismo, en colaboración con la Comisión Nacional de Estadística Judicial, con el objetivo de concretar datos sobre las comunicaciones efectuadas por los sujetos obligados. Esta encomienda obedece, en primer término, a la correspondencia con la demanda impuesta por la normativa internacional[22]. Y, en segundo término, también es una fuente de información clave para la mejora del régimen de lucha contra el blanqueo de capitales y la financiación del terrorismo. Todo ello permite conocer el grado de cumplimiento efectivo con los estándares normativos internacionales y nacionales contra el blanqueo de capitales y la financiación del terrorismo[23].

## 3.2. El Comité Permanente de la Comisión

Como órgano ejecutivo de la Comisión le corresponde la orientación de la actuación del SEPBLAC y la aprobación de su organización y funcionamiento[24]; la aprobación, a propuesta del SEPBLAC y, en caso de convenio, de los órganos de supervisión de las entidades financieras, del Plan Anual de Inspección de los sujetos obligados; así como la formulación de requerimientos a los sujetos obligados relativos al cumplimiento de las obligaciones de la Ley 10/2010, de 28 de abril[25]. Estas funciones responden a la pretensión de instaurar un régimen que, en todo caso, se interrelacione con la actuación de los órganos judiciales, el Ministerio Fiscal y la Policía Judicial en orden a la prevención de la utilización del sistema financiero para el blanqueo de capitales[26].

El Plan Anual de Inspección, cuya aprobación corresponde al Comité Permanente, se trata del documento en el que se recogen las actividades de inspección a modo de policía administrativa que desarrolla el SEPBLAC[27]. Las actuaciones no recogidas en el Plan Anual de Inspección requieren de una aprobación particular por el Comité Permanente[28]. Los resultados de las actuaciones de investigación llevadas a cabo por el SEPBLAC, o por los supervisores de las instituciones financieras en caso de convenio, se remiten a la Secretaría de la Comisión, que las eleva a consideración del Comité Permanente. También el SEPBLAC puede proponer a este la formulación de requerimientos a los sujetos obligados para la toma de medidas de corrección.

22. Véase artículo 44 de la Directiva 2015/849, de 20 de mayo y Recomendación n.º 33 del GAFI.
23. Úbeda Martínez-Valera, P., *op. cit.*, pág. 307.
24. Véase artículo 45.3 de la Ley 10/2010, de 28 de abril.
25. Véase artículo 64.1 del Real Decreto 304/2014, de 5 de mayo.
26. Úbeda Martínez-Valera, P.: *op. cit.*, pág. 309.
27. Alcaraz Lamana, C., *op. cit.*, pág. 30.
28. *Idem.*

El Comité Permanente está presidido por el director general del Tesoro y Política Financiera que, a su vez, se acompaña de toda una serie de vocales[29]. Entre estos últimos destacamos un representante del Banco de España, de la CNMV, de la Secretaría de Estado de Seguridad, de la Dirección General de la Policía, de la Dirección General de la Guardia Civil, de la Fiscalía Antidroga, así como del Departamento de Inspección Financiera y Tributaria de la Agencia Estatal de la Administración Tributaria (AEAT). La condición de miembro del Comité Permanente no requiere la correlativa en el Pleno, exigiéndose únicamente que la persona nombrada haya adquirido el rango de subdirector general o equivalente.

## 3.3. El Comité de Inteligencia Financiera

A este nuevo órgano dependiente de la Comisión de Prevención del Blanqueo de Capitales e Infracciones Monetarias se le atribuye, como funciones generales, la promoción del análisis y la formación de inteligencia financiera por el SEPBLAC, así como la puesta a disposición de dicha información en favor de los sujetos obligados, ya bien sea de forma directa o a través de las asociaciones profesionales. Los motivos de su creación se relacionan con la prestación del debido apoyo a las funciones de inteligencia financiera que desarrolla el SEPBLAC, al mismo tiempo que se promueva una coordinación clave en la lucha contra el blanqueo de capitales y la financiación del terrorismo.

Otras atribuciones específicas del Comité de Inteligencia Financiera son las siguientes. En primer lugar, la aprobación de toda una serie de aspectos que requieren de una propuesta previa por el SEPBLAC: los criterios generales de difusión de los informes de inteligencia financiera, las orientaciones y directrices generales en materia de análisis e inteligencia financieros, y las directrices a los sujetos obligados en materia de comunicación de operaciones por indicio. En segundo lugar, el apoyo para la retroalimentación entre el SEPBLAC y las instituciones receptoras de la inteligencia financiera. Y, en tercer lugar, la elaboración de estudios de tipologías sobre blanqueo de capitales y financiación del terrorismo tras el análisis estratégico completado por el SEPBLAC[30].

El Comité de Inteligencia Financiera, en línea con la estructura de la Comisión, adquiere una formación diversa en la que se representan los distintos sectores del estado vinculados con la inteligencia financiera, el análisis criminal y la supervisión, bajo la presidencia del director general del Tesoro y Política Financiera. Se agrupan en el Comité de Inteligencia Financiera, entre otros, un representante de la Fiscalía Antidroga, de la Fiscalía de la Audiencia Nacional, del Banco de España, de la Dirección General de la Policía, de la Dirección

29. Véase artículo 64.2 del Real Decreto 304/2014, de 5 de mayo.

30. Véase artículo 65.1 del Real Decreto 304/2014, de 5 de mayo.

General de la Guardia Civil, del CNI, así como el director del SEPBLAC y el subdirector general de Inspección y Control de Movimientos de Capitales.

La condición de miembro en el Comité de Inteligencia Financiera no necesita estar acompañada de la adquisición de la condición de miembro del Pleno. El extremo más relevante es que todas aquellas representaciones de las distintas estructuras del estado que forman parte del Comité de Inteligencia Financiera cumplan con el requisito de tratarse de representantes con el rango mínimo de subdirector general o equivalente[31]. Ello instaura la máxima de que las decisiones tomadas para el cumplimiento de funciones por la normativa de prevención de blanqueo de capitales se deben adoptar por las máximas representaciones de las instituciones estatales.

# 4. Los órganos de apoyo de la Comisión de Prevención del Blanqueo de Capitales e Infracciones Monetarias

## 4.1. La Secretaría de la Comisión

Es el primer órgano de apoyo a la Comisión de Prevención del Blanqueo de Capitales e Infracciones Monetarias previsto en la Ley 10/2010, de 28 de abril, cuyas funciones se llevan a cabo por la Subdirección General de Inspección y Control de Movimientos de Capitales, dependiente de la Dirección General del Tesoro y Política Financiera, dentro del organigrama de la Secretaría de Estado de la Economía y Apoyo a la Empresa (Ministerio de Economía, Comercio y Empresa). Su titular ostenta, con carácter nato, la condición de secretario y vocal de la Comisión y de sus Comités. Estamos ante un órgano técnico y administrativo, que presta apoyo a las subdivisiones orgánicas de la Comisión.

Bajo la premisa de auxilio a la Comisión, la Secretaría se encarga de las siguientes tareas: la realización de las actuaciones previas necesarias a la incoación de los procedimientos sancionadores por infracción de las obligaciones previstas en la Ley 10/2010, de 28 de abril; la propuesta al Comité Permanente de la incoación y el sobreseimiento de los procedimientos sancionadores, salvo en los procedimientos sancionadores por incumplimiento de la obligación de declaración de movimientos de medios de pago; la instrucción de los procedimientos sancionadores por infracciones previstas en la Ley 10/2010, de 28 de abril; y elevar a quien corresponda la propuesta de resolución de los procedimientos sancionadores a que hubiere lugar por la comisión de infracciones en la Ley 10/2010, de 28 de abril.

31. Úbeda Martínez-Valera, P., *op. cit.*, pág. 302.

Las funciones señaladas permiten destacar la naturaleza administrativa de la Secretaría, lo cual se considera como un elemento de diferenciación respecto al SEPBLAC[32]. A la Secretaría de la Comisión corresponden las tareas de apoyo en relación con los procedimientos administrativos sancionadores, como el acuerdo de actuaciones previas a la incoación, la instrucción de los procedimientos sancionadores, la adopción de propuestas de incoación y de sobreseimiento, o la formulación de propuestas de resolución, bien elevándose aquellas al Comité Permanente en relación con las infracciones graves y muy graves, bien al director general del Tesoro y Política Financiera en las infracciones leves, ambas contempladas en la Ley 10/2010, de 28 de abril.

La Secretaría se establece como el órgano de referencia para la remisión de información sobre posibles infracciones de las obligaciones contenidas en la Ley 10/2010, de 28 de abril. El Banco de España, la CNMV, la DGSFP, la Dirección General de los Registros y del Notariado, el Instituto de Contabilidad y Auditoría de Cuentas, los colegios profesionales y otros órganos estatales o autonómicos competentes, deben informar razonadamente a la Secretaría de movimientos sospechosos detectados en su labor inspectora o supervisora.

## 4.2. El SEPBLAC como UIF nacional

### 4.2.1. La demanda de creación por la normativa internacional

El establecimiento de UIF como agencias para la recepción y el análisis de los informes de operaciones sospechosas realizados por los sujetos obligados se ha convertido en un constante reclamo de las organizaciones internacionales centradas en la lucha contra el blanqueo de capitales. El objetivo es que tales unidades colaboren con las autoridades competentes de la investigación y el enjuiciamiento, sobre todo mediante la transmisión de información[33]. Entre los actores más insistentes en punto al establecimiento de UIF destaca el GAFI. Las políticas de esta organización imponen una serie de deberes a los sujetos obligados, entre los que se halla la comunicación de operaciones sospechas para su posterior análisis por las UIF nacionales.

En el ámbito de Naciones Unidas también se ha promovido la creación de UIF como estructuras esenciales en la prevención del blanqueo de capitales. Destacamos, en primer lugar, la Convención de Palermo contra delincuencia organizada transnacional del 2000, que incluye un régimen dual contra el blanqueo de capitales y, entre las medidas preventivas, reafirma la necesidad

32. Úbeda Martínez-Valera, P., *op. cit.*, pág. 312.

33. De la Torre Lascano, M., *Lavado de activos: estudio sobre la prevención (en especial referencia al caso ecuatoriano)*. Tirant lo Blanch, Valencia, 2020, pág. 101.

de que los estados establezcan UIF como órganos encargados de analizar y difundir información sobre actividades de blanqueo de capitales y otros delitos financieros. Esta premisa se acompaña de una declaración tendente al mayor intercambio de información como ejemplo de la cooperación internacional necesaria para hacer frente a la criminalidad organizada[34].

También en sede de Naciones Unidas debemos mencionar el Programa Mundial contra el blanqueo de capitales, el producto del delito y la financiación del terrorismo, que se inserta en la agenda de la Unidad contra el blanqueo de capitales de la Oficina de las Naciones Unidas contra la Droga y el Delito. Uno de los objetivos perseguidos consiste en la consolidación de las UIF como entidades centrales para el análisis y la difusión a las autoridades competentes de información financiera. Por ello, se reclama de los estados las herramientas necesarias en favor de las UIF para que estas puedan recopilar, analizar y difundir información financiera a nivel nacional e internacional[35].

La creación de UIF como estructuras esenciales para la lucha contra el blanqueo de capitales y la financiación del terrorismo es una máxima que también se ha reconocido en el ámbito del Consejo de Europa. Nos remitimos a lo dispuesto en el Convenio de Varsovia de 2005, que también a lo largo de sus disposiciones hace referencia a la debida creación de agencias de inteligencia financiera por cada estado. En línea con lo reclamado por el Programa Mundial de Naciones Unidas, el texto del Consejo de Europa acompaña la anterior previsión general comentada de una derivada esencial, como es la dotación de capacidad suficiente a las UIF para acceder, directa o indirectamente, a la información de las entidades financieras[36].

### 4.2.2. El intercambio de información financiera en la Unión Europea

El escaso intercambio de información entre las agencias nacionales de inteligencia financiera ha constituido una de las principales problemáticas sobre las que la acción comunitaria europea ha incidido en mayor medida con la finalidad de lograr un régimen normativo para el cumplimiento de la máxima enunciada. La necesidad de que cada estado crease una UIF se determinó originalmente en la Directiva 91/308/CEE, de 10 de junio, bajo la fórmula «autoridades responsables de la lucha contra el blanqueo de capi-

34. Urbaneja Cillán, J., «Acciones contra el blanqueo de capitales en el marco latinoamericano y caribeño», en *Anuario de la Facultad de Derecho de la Universidad de Extremadura*, n.º 29, 2011, pág. 210.

35. Mcdonell, R., «UN Anti-Money Laundering Initiatives», en Muller, W. H.; Kälin, C. H.; y Goldsworth, J. G. (eds.): *Anti-Money Laundering: International Law and Practice*. Wiley Editorial, Chichester, 2007, pág. 53.

36. Álvarez Pastor, D., Eguidazu Palacios, F., *Manual de prevención del blanqueo de capitales*. Marcial Pons, Madrid, 2007, pág. 72.

tales»[37]. También la Directiva 2001/97/CE, de 4 de diciembre, adopta dicha fórmula indeterminada. No obstante, entre medias se adoptó la Decisión 2000/642/JAI, de 17 de octubre, que tenía por objetivo afrontar la falta de intercambio de información entre las UIF de los estados miembros.

Para completar un régimen amplio de intercambio de información, en la Decisión 2000/642/JAI, de 17 de octubre, se estipuló que la negativa a las solicitudes de información solo podía obedecer a la creación de una situación de obstrucción a la labor de investigación desarrollada por la UIF requerida, a una desproporción evidente en los datos requeridos en ponderación con las metas perseguidas o a la vulneración de principios básicos del estado requerido[38]. Este régimen amplio en el envío de información financiera se reforzó con la creación de FIU.net, una plataforma informática descentralizada para el intercambio de información entre las agencias nacionales[39].

La Directiva 2005/60/CE, de 26 de octubre, dio un paso adelante en el papel que debían ejercer las UIF. Estas se definen como los centros nacionales encargados de la recepción, el análisis y la divulgación a las autoridades competentes de transacciones sospechosas de blanqueo de capitales o financiación del terrorismo. Uno de los aspectos declarados como esenciales en la nueva norma consistía en que la solicitud de datos por las UIF o el acceso a los registros de las instituciones financieras para el desarrollo de investigaciones posteriores debía estar sujeto al menor número de obstáculos.

La Directiva 2015/849, de 20 de mayo, modificada tres años más tarde por la Directiva 2018/843, de 30 de mayo, incide nuevamente en la necesidad de que las UIF estén facultadas para realizar intercambios de información sin obstáculos, previa solicitud de otras entidades homólogas. Para lograr investigaciones eficaces, la norma establece que en la solicitud de información deben hacerse constar los hechos antecedentes, las razones y las finalidades perseguidas con la obtención de la información. Esta última deberá ponerse a disposición a través de los mecanismos de comunicación acordados entre las agencias nacionales o mediante FIU.net. Únicamente en casos excepcionales se podrá denegar el intercambio de información.

Las normas de la Unión Europea expuestas hasta el momento habían tratado de instaurar un régimen amplio de intercambio de información entre

37. Úbeda Martínez-Valera, P., *op. cit.*, pág. 317.

38. Pérez Marín, M. Á., «Las unidades de inteligencia financiera: el intercambio de información como medio para la prevención, la investigación y el enjuiciamiento de la delincuencia económica vinculada con el terrorismo», en Jimeno Bulnes, M. (dir.): *La evolución del espacio judicial europeo en materia civil y penal: su influencia en el proceso español*. Tirant lo Blanch, Valencia, 2022, pág. 366.

39. Carrillo del Teso, A. E., «Unidades de inteligencia financiera: las TICs en la prevención del blanqueo de capitales», en Pérez Álvarez, F. (ed.): *Moderno discurso penal y nuevas tecnologías: memorias [del] III Congreso Internacional de Jóvenes Investigadores en Ciencias Penales, 17, 18 y 19 de junio de 2013*. Ediciones Aquilafuente, Salamanca, 2014, pág. 193.

las UIF. No obstante, las investigaciones financieras todavía resultaban de escasa transcendencia en la medida en que las instituciones bancarias se configuraban en la práctica como refugios seguros para los activos ilícitos, lejos del alcance por las autoridades judiciales. Este hecho propició que se aprobase la Directiva 2019/1153, de 20 de junio, por la que se establecen normas destinadas a facilitar el uso de información financiera y de otro tipo para la prevención, detección, investigación o enjuiciamiento de infracciones penales y por la que se derogó la Decisión 2000/642/JAI, de 17 de octubre.

El nuevo texto normativo surgió en un contexto de preocupación tras el escándalo generado tras la salida a la luz de los *Panamá Papers*, que demostraron el escaso intercambio de información entre las UIF nacionales. Mediante la Directiva 2019/1153, de 20 de junio, los estados miembros deben autorizar a ciertas autoridades nacionales para el acceso directo a los registros e informaciones contenidos en las UIF, así como para formular requerimientos que solo se podrán denegar en casos excepcionales. El objetivo es lograr una identificación más rápida de las cuentas bancarias de las organizaciones criminales, especialmente aquellas vinculadas a actividades de terrorismo,

En el marco comunitario hemos de mencionar finalmente la reciente Directiva 2024/1640, de 31 de mayo, que también subraya el papel esencial que deben desarrollar las UIF como agencias independientes y autónomas para la recepción y el análisis de la información, esto es, la creación de inteligencia financiera. Uno de los extremos en los que incide el texto comunitario es la autonomía operativa de la que deben disponer las UIF, que no pueden verse sometidas en su actividad a injerencias políticas, gubernamentales o industriales indebidas que puedan comprometer su libre ejercicio[40].

### 4.2.3. El Grupo Egmont para el intercambio de información financiera

La creación del Grupo Egmont respondió a la idea de configurar una plataforma informal e internacional que fomente la cooperación entre las agencias de inteligencia financiera con el fin de lograr operativos intercambios de información y asistencia técnica. El propio GAFI reconoce la importancia de que las UIF se agrupen en una estructura de integración sobre inteligencia financiera; por ello, impone a los países que soliciten la membresía de sus UIF en el Grupo Egmont. Más en concreto, en el Apartado G) de la Nota Interpretativa a la Recomendación n.º 29 del GAFI se reclama a los estados para que cumplan con la solicitud de acceso, tras garantizar que las estructuras nacionales de inteligencia financiera cumplan con la Declaración de Propósito del Grupo Egmont y sus Principios para el Intercambio de Información.

40. Véase Considerando 64 de la Directiva 2024/1640, de 31 de mayo.

La génesis del Grupo Egmont en 1995 traía causa de la necesidad de establecer un órgano de referencia que ayudase a los estados a articular un régimen amplio de intercambio de información[41]. Se trata de auxiliar a las plataformas nacionales de inteligencia financiera para lograr intercambios de información sistematizados, así como para conseguir la adecuada formación del personal adscrito para que desarrollen su actividad conforme a las premisas de máxima efectividad y cumplimiento. Para el logro de tales objetivos, el Grupo Egmont se compone de un Comité y diferentes grupos de trabajo (sobre intercambio de información, sobre membresía, apoyo y cumplimiento, sobre políticas y procedimientos y de asistencia técnica y capacitación).

El Grupo Egmont ha experimentado una transformación notable que se puede constatar en la subdivisión funcional. A ello se suma la colaboración o participación como miembro u observador en otras estructuras; así ocurre en el caso de CARIN, que se trata de otra red informal de cooperación interinstitucional que auxilia a los estados en la aplicación del decomiso, la localización de bienes y la recuperación de activos, a su vez en cooperación con Eurojust y Europol como miembros permanentes en su secretariado[42]. Ello muestra un ejemplo representativo de la diversificación alcanzada con la finalidad de auxiliar a las estructuras nacionales de inteligencia financiera para lograr un régimen amplio de intercambio de información.

Los objetivos del Grupo Egmont se sintetizan en los siguientes. En primer lugar, el diseño, la sistematización y la puesta a disposición de las UIF de canales efectivos para el intercambio de información sobre la base de los principios de reciprocidad, finalidad y cumplimiento de las prescripciones legales[43]. En segundo lugar, el auxilio a los estados en punto a la formación del personal adscrito a las UIF. En tercer lugar, la colaboración con las agencias nacionales para una estructuración de las operaciones mediante divisiones de trabajo efectivas. Y, en cuarto lugar, la promoción de un mayor régimen de comunicación entre UIF mediante el uso de nuevas tecnologías[44].

La Egmont Secure Web responde precisamente a la última de las metas enunciadas. Consiste en un mecanismo electrónico verificado con patrones de seguridad en el que las UIF pueden realizar solicitudes y entregas de información. Su utilización es posible para los miembros del Grupo Egmont y se define como un buzón electrónico para intercambiar información a través de correos cifrados y comunicaciones internas. No obstante, su falta de sofis-

41. Nieto Martín, A., «Transformaciones del Ius Puniendi en el derecho global», en Nieto Martín, A. y García Moreno, B. (dirs.): *Ius puniendi y global law: Hacia un derecho penal sin estado*. Tirant lo Blanch, Valencia, 2019, pág. 41.

42. *Idem.*

43. Muller, W. H., «The Egmont Group», en Muller, W. H.; Kälin, C. H. y Goldsworth, J. G. (eds.): *Anti-Money Laundering: International Law and Practice*. Wiley Editorial, Chichester, 2007, pág. 90.

44. De la Torre Lascano, M., *op. cit.*, pág. 123.

ticación y la desconexión de algunos países plantean una cierta demanda relativa a una fusión con FIU.net[45]. El Grupo Egmont ha recogido esta reclamación y aborda en la actualidad una posible integración entre plataformas.

En definitiva, el Grupo Egmont, mediante sus actividades, trata de lograr unos esquemas de comunicación rápidos entre las UIF, para lo cual las nuevas tecnologías desarrollan un papel esencial. Su actividad se dirige a conseguir el establecimiento de canales de cooperación entre las UIF para un intercambio rápido de información. El Grupo Egmont desarrolla reuniones periódicas y pone a disposición de las agencias nacionales diferentes recursos para completar un régimen que propicie un amplio intercambio de información. Este último debe ajustarse, en todo caso a los principios de libre intercambio de información, reciprocidad, inmediatez, limitación en el uso de aquella bajo el consentimiento de la web suministradora y confidencialidad de la información[46].

### 4.2.4. Régimen y estructura

El SEPBLAC constituye uno de los órganos de apoyo de la Comisión de Prevención del Blanqueo de Capitales e Infracciones Monetarias, que se trata de un organismo autónomo bajo la Secretaría de Estado de Economía y Apoyo a la Empresa. El SEPBLAC, en último término, se inserta en el organigrama del Ministerio de Economía, Comercio y Empresa. Sus áreas funcionales se agrupan en Inteligencia Financiera, Planificación y Supervisión e Inspección. La actividad del Servicio Ejecutivo alcanza a la totalidad del territorio nacional[47].

El Banco de España se encarga de la gestión presupuestaria del SEPBLAC, sobre la base de legislación específica y acuerdos celebrados entre las partes. No obstante, la aprobación del presupuesto del SEPBLAC corresponde a la Comisión, que luego forma parte de la propuesta de presupuesto de gastos de funcionamiento e inversiones a que se refiere el artículo 4.2 de la Ley 13/1994, de 1 de junio, de autonomía del Banco de España. Los gastos que contra el citado presupuesto se realicen serán atendidos por el Banco de España, que se resarcirá conforme a lo previsto legalmente[48].

El SEPBLAC coopera con la Comisión de Vigilancia de Actividades de Financiación del Terrorismo (CVAFT)[49]. Esta entidad, adscrita al Ministerio

45. Deleanu, I., Van Den Broek, M., «International cooperation», en VV. AA.: *The Economic and Legal Effectiveness of the European Union´s Anti-Money Laundering Policy*. Edward Elgar Publishing, Cheltenham, 2014, pág. 153.

46. Jiménez García, F., *La prevención y lucha contra el blanqueo de capitales y la corrupción: Interacciones evolutivas en un derecho internacional global*. Comares, Granada, 2015, pág. 235.

47. Véase art. 67.1 primer párrafo del Real Decreto 304/2014, de 5 de mayo.

48. Llavador Piqueras, J., Llavador Cisternes, H., *op. cit.,* pág. 411.

49. Alcaraz Lamana, C., *op. cit.*, pág. 8.

del Interior. fue creada mediante la Ley 12/2003, de 21 de mayo. El director del SEPBLAC asiste a las reuniones de la CVAFT. Esta última puede adoptar decisiones destinadas al bloqueo de fondos o transacciones por las sospechas de vinculación con operaciones de financiación del terrorismo, al igual que puede proceder a la liberación de fondos bloqueados, todo ello en el marco de un trabajo cooperativo con las autoridades judiciales[50]. El SEPBLAC reduce su función a una cooperación con la CVAFT para la notificación a los sujetos obligados de la congelación de activos[51].

No debe confundirse al SEPBLAC con otros órganos de inteligencia en España. En materia de financiación del terrorismo distinguíamos hasta tiempos recientes un órgano autónomo, el Centro Nacional de Coordinación Antiterrorista (CNCA). Su creación se produjo tras los atentados del 11 de marzo de 2004 en Madrid. A dicho órgano de inteligencia se le atribuía la prevención, el seguimiento y el análisis de las amenazas terroristas en el territorio nacional. Más en concreto, sus funciones se vinculaban a la revisión de información relacionada con el terrorismo, a la coordinación de actuaciones preventivas frente a aquel y al establecimiento de los niveles de alerta en España.

También en 2006 se estableció en la estructura nacional un órgano centrado en la optimización de la lucha contra el crimen organizado, conocido como el Centro de Inteligencia contra el Crimen Organizado (CICO). La decisión de crear esta entidad obedeció a la necesidad de que las Fuerzas y Cuerpos de Seguridad del Estado actuasen coordinadamente frente a fenómenos propios del crimen organizado, como el narcotráfico, el tráfico de seres humanos o de armas. Entre las funciones atribuidas a la CICO destacamos, de un lado, el análisis de la información procedente de la Policía Nacional, la Guardia Civil o la Vigilancia Aduanera. Y, de otro, la cooperación internacional con Europol, Interpol y otros organismos nacionales de inteligencia.

La fusión del CNCA y el CICO en 2014 dio lugar al actual Centro de Inteligencia contra el Terrorismo y el Crimen Organizado (CITCO), dependiente del Ministerio del Interior. Bajo esta entidad se centraliza la coordinación de la información y actuaciones en materia de financiación del terrorismo, crimen organizado y radicalización violenta. Entre las funciones del CITCO podemos indicar las siguientes: el desarrollo un análisis estratégico en las materias enunciadas; el aseguramiento de una coordinación efectiva entre las Fuerzas y Cuerpos de Seguridad del Estado; la gestión de los niveles de alerta antiterrorista; y la confección de inteligencia estratégica sobre la que se adoptan posteriores decisiones políticas y de seguridad.

El SEPBLAC sigue el modelo de UIF de corte administrativo. Su estructura se incardina bajo la Comisión de Prevención del Blanqueo de Capitales e Infracciones Monetarias, adscrita a la Secretaría de Estado de Economía y

50. Carlos de Oliveira, A. C., *op. cit.*, pág. 430.

51. *Idem.*

Apoyo a la Empresa. La vinculación del SEPBLAC con el Banco de España, que hasta fechas recientes ejercía la dirección de aquel, evidencia la naturaleza de este órgano de apoyo a la Comisión. No obstante, la decisión de adoptar un órgano de naturaleza administrativa no menoscaba la independencia y la autonomía operativas que debe presidir toda actuación del SEPBLAC como órgano perteneciente a la comunidad de inteligencia financiera en España.

En la estructura del SEPBLAC se hallan representados la Secretaría de Estado de Seguridad del Ministerio del Interior, la Dirección General de la Policía y de la Guardia Civil, el Departamento de Aduanas y el CNI[52]. Asimismo, se engloba la Unidad de Inteligencia Financiera de la AEAT y, en calidad de unidades policiales adscritas, la Unidad de Investigación de la Guardia Civil y la Brigada Central de Inteligencia Financiera del Cuerpo Nacional de Policía[53]. A esta última, que forma parte de la Unidad Central de Delincuencia Económica y Fiscal de la Policía Nacional, corresponde la investigación y la persecución de actos de blanqueo de capitales[54]. Esta composición aproxima al SEPBLAC a la categoría de UIF policial o judicial, frente a su definición como administrativa.

El personal laboral del SEPBLAC percibe sus retribuciones con cargo al presupuesto general del organismo. La vinculación laboral se rige por una relación de derecho laboral. Los procedimientos de contratación, que exigen la previa autorización de la Comisión, tienen carácter competitivo y se basan en los principios de mérito y capacidad[55]. El personal laboral no tiene la condición de Policía Judicial[56]. Tampoco se les otorga la condición de agentes de la autoridad, salvo en sus actuaciones sobre infracciones de la Ley 10/2010, de 28 de abril[57].

### 4.2.5. Atribuciones

El SEPBLAC ejerce toda una serie de funciones para la prevención del blanqueo de capitales y de la financiación del terrorismo. Entre ellas, auxilia a los órganos judiciales, al Ministerio Fiscal, a la Policía Judicial y a los órganos administrativos; remite a los órganos judiciales, al Ministerio Fiscal o a la Policía Judicial las actuaciones de las que se deriven indicios de delito; recibe las comunicaciones por indicios; analiza la información recibida por los sujetos obligados; ejecuta las órdenes de la Comisión o de su Comité Permanente;

52. Alcaraz Lamana, C., *op. cit.*, pág. 9.

53. Véase artículo 68 del Real Decreto 304/2014, de 5 de mayo.

54. Llavador Piqueras, J., Llavador Cisternes, H., *op. cit.,* pág. 429.

55. Véase artículo 67.7 párrafo tercero del Real Decreto 304/2014, de 5 de mayo.

56. Alcaraz Lamana, C., *op. cit.*, pág. 11.

57. *Idem.*

inspecciona el cumplimiento por los sujetos obligados de las medidas de prevención del blanqueo de capitales; y propone al Comité Permanente la formulación de requerimientos a los sujetos obligados[58].

La primera de las funciones del SEPBLAC en la que nos detenemos es la recepción y el análisis de los reportes de operaciones sospechosas que deben realizar los sujetos obligados. Este cometido se estipula por la misma normativa internacional y permite señalar el papel elemental que se atribuye a las agencias de inteligencia financiera en la lucha contra el blanqueo de capitales. Tras el análisis de los informes sobre operaciones sospechosas, el SEPBLAC y sus entidades homólogas en el extranjero elaboran una inteligencia financiera básica para las autoridades encargadas de la investigación y la persecución del delito.

El SEPBLAC analiza la información recibida de los sujetos obligados y, en caso de indicios o certezas de blanqueo de capitales, delitos antecedentes o financiación del terrorismo, remite el informe de inteligencia financiera, de forma autónoma o tras la petición de las autoridades, al Ministerio Fiscal o a las autoridades judiciales, policiales o administrativas[59]. El análisis que se le atribuye debe ser desarrollado de forma libre y con la suficiente capacidad autónoma para analizar, pedir o transmitir información. Los informes de inteligencia tienen la consideración de confidenciales. Tampoco puede ser objeto de revelación la identidad de los analistas y de los funcionarios que comunicaron la existencia de indicios a los órganos de control interno del sujeto obligado[60].

Las comunicaciones de los sujetos obligados se canalizan a través de un procedimiento de diversas fases en orden a su análisis minucioso. En primer lugar, una fase de registro en el que toda la información recibida por el SEPBLAC se registra e integra en la aplicación TAIS. En segundo lugar, una fase de valoración inicial para determinar la necesidad de su posterior asignación a una de las áreas de servicio del SEPBLAC. En caso de decidirse por la distribución del caso, en la fase de atribución se envía el contenido a algunas de las unidades internas para posteriores averiguaciones y la elaboración de un informe. Finalmente, la fase de remisión consiste en la puesta a disposición de la inteligencia financiera en favor de las autoridades judiciales, policiales o administrativas competentes.

Tras el análisis de la información y la elaboración de los informes de inteligencia financiera, el SEPBLAC utiliza canales protegidos, seguros y exclusivos para la remisión de la información[61]. Este envío se produce ante la constatación de indicios o certezas de blanqueo de capitales o financiación del terrorismo.

58. Véase artículo 45.4 de la Ley 10/2010, de 28 de abril.

59. Véase artículo 46.1 párrafo primero de la Ley 10/2010, de 28 de abril.

60. Véase artículo 46.1 párrafo segundo de la Ley 10/2010, de 28 de abril.

61. Véase artículo 67.4 del Real Decreto 304/2014, de 5 de mayo.

Los destinatarios de la inteligencia financiera son los órganos de investigación competentes (Policía Nacional, Guardia Civil, Ministerio Fiscal, órganos judiciales y AEAT) u otras autoridades supervisoras (si la información es relevante para la supervisión financiera). No obstante, a ello se añaden otras UIF de estados miembros de la Unión Europea[62] o incluso de terceros países sobre la base de memorandos de entendimiento o los principios del Grupo Egmont.

La Ley 10/2010, de 28 de abril, proscribe la incorporación directa de los informes de inteligencia financiera a las diligencias judiciales o administrativas[63]. Ello supone que los informes de inteligencia financiera únicamente se pueden considerar como diligencias de investigación que permiten iniciar actuaciones ante los órganos judiciales o administrativos competentes[64]. La información financiera es objeto de remisión al Ministerio Fiscal o a las autoridades judiciales o administrativas como primeros elementos para el desarrollo de investigaciones ulteriores, si bien nunca pueden ser considerados a efectos probatorios. La sentencia definitiva que se adopte no puede estar fundamentada en dicha información financiera, dado que el legislador rechaza atribuirle valor de prueba.

Cuando así se requiera por una UIF de un estado miembro de la Unión Europea, el SEPBLAC tiene facultades para suspender una transacción en curso al relacionarse con posibles operaciones de blanqueo de capitales o financiación del terrorismo. El objetivo es que la agencia de inteligencia financiera de otro estado pueda proceder al análisis de la transacción, confirmar la sospecha de delito y proceder a la remisión de tal conclusión a las autoridades competentes. En el caso de que la suspensión de transacciones se relacione con indicios de financiación del terrorismo, se debe informar a la Secretaría de la CVAFT, previa autorización de la UIF requirente. El período máximo de suspensión será de un mes, salvo ratificación o prórroga judicial a solicitud del Ministerio Fiscal.

También el SEPBLAC desarrolla una función de supervisión del cumplimiento por los sujetos obligados de las medidas de prevención[65]. Para ello puede llevar a cabo cualesquiera actuaciones inspectoras que estime procedente[66]. Como resultado de las actuaciones de inspección se adopta un

62. El intercambio de información financiera entre las agencias nacionales de estados miembros de la Unión Europea se rige por los artículos 51 a 57 de la Directiva 2015/849, de 20 de mayo.

63. Véase artículo 46.1 párrafo tercero de la Ley 10/2010, de 28 de abril.

64. González Cussac, J. L.; Larriba Hinojar, B.; Fernández Hernández, A., «Capítulo 19. Los servicios de inteligencia en el Derecho español», en González Cussac, J. L. (coord..): *Inteligencia*. Tirant lo Blanch, Valencia, 2012, pág. 360.

65. Véase artículo 45.4 letra f) de la Ley 10/201, de 28 de abril.

66. Blasco Díaz, J. L., «Capítulo VII. La organización institucional», en Vidales Rodríguez, C. (dir.): *Régimen jurídico de la prevención y represión del blanqueo de capitales*. Tirant lo Blanch, Valencia, 2015, pág. 269.

informe en el que se recogen los actos de comprobación y las recomendaciones para la adecuación de las medidas de control interno establecidas por los sujetos obligados conforme a la Ley 10/2010, de 28 de abril. Los sujetos obligados deben elaborar un plan de acción a los efectos de incorporar su contenido, señalando plazos de implementación y forma de aplicación de cada medida.

Los sujetos obligados, así como sus empleados, directivos y agentes, deben prestar en todo momento la máxima colaboración con el SEPBLAC[67]. En esta máxima se incluye la presentación de los documentos o informes que sean necesarios, como pueden ser libros de asientos contables, archivos digitales, registros, programas informáticos, comunicaciones internas o actas[68].

Los informes de inspección tienen valor probatorio en el procedimiento sancionador ante la Comisión[69], sin perjuicio de las pruebas que en su descargo puedan presentar las partes para hacer valer sus derechos o intereses[70].

El SEPBLAC realiza igualmente funciones de análisis estratégico para identificar patrones, tendencias y tipologías, de los que informará al Comité de Inteligencia Financiera. Este último debe determinar posibles amenazas y vulnerabilidades en un análisis de riesgo que dará forma a las políticas de prevención del blanqueo de capitales y la financiación del terrorismo. En todo caso, la información recibida, procesada o difundida por el SEPBBLAC debe ser objeto de protección adecuada, especialmente en punto a su seguridad y confidencialidad, por lo que se deben respetar los procedimientos para el manejo, el archivo, la difusión y la protección de la información.

Finalmente, se atribuye al SEPBLAC la gestión del Fichero de Titularidades Financieras. En éste se agrupa la información sobre cuentas de ahorro, cuentas de valores y depósitos a plazo remitida por las entidades de crédito. El Fichero es responsabilidad de la Secretaría de Estado de Economía y Apoyo a la Empresa, pero su gestión se atribuye al SEPBLAC. Corresponde a este el establecimiento de los procedimientos técnicos de consulta del Fichero[71]. Estamos ante un mecanismo en el que se contiene información financiera y que complementa la actividad del SEPBLAC[72], que asimismo realiza un registro de las consultas y accesos desde los puntos de acceso.

67. Véase artículo 47.4 de la Ley 10/2010, de 28 de abril

68. Alcaraz Lamana, C., *op. cit.*, pág. 31.

69. Carlos de Oliveira, A. C., *op. cit.*, pág. 468.

70. Véase artículo 47.6 de la Ley 10/2010, de 28 de abril.

71. Véase artículo 52 del Real Decreto 304/2014, de 5 de mayo.

72. Úbeda Martínez-Valera, P., *op. cit.*, pág. 375.

## 5. A modo de recapitulación

La derogada Ley 19/1993, de 28 de diciembre, creó en su momento la Comisión de Prevención del Blanqueo de Capitales e Infracciones Monetarias. Este organismo se recoge en la legislación actual, cuya regulación se comprende en los artículos 44 y ss. de la Ley 10/2010, de 28 de abril, y en los artículos 62 y ss. del Real Decreto 304/2014, de 5 de mayo.

La Comisión depende de la Secretaría de Estado de Economía y Apoyo a la Empresa. Se trata de un órgano colegiado que, junto a sus comités, se reúne con carácter general dos veces al año, sin perjuicio de convocatorias adicionales. Puede actuar en Pleno o a través de su Comité Permanente, en el que se integran representantes políticos, policiales y judiciales. En particular, en el Pleno se integran hasta 25 miembros, como el secretario de Estado de Economía, el director general del Tesoro, el fiscal de sala jefe de la Fiscalía Antidroga, el secretario general del Banco de España, el director de inteligencia del CNI o el general jefe de Policía Judicial de la Guardia Civil.

Las funciones de la Comisión son, a modo de resumen, las siguientes. En primer lugar, la dirección de las actividades de prevención de la utilización del sistema financiero o de otros sectores de actividad económica para el blanqueo de capitales y la financiación del terrorismo. En segundo lugar, la colaboración con las Fuerzas y Cuerpos de Seguridad, coordinando las actividades de investigación y prevención llevadas a cabo por los órganos de las Administraciones Públicas. En tercer lugar, el auxilio a los órganos judiciales, al Ministerio Fiscal y a la Policía Judicial. En cuarto lugar, el nombramiento y el cese del director del SEPBLAC, previa consulta con el Banco de España. Y, en quinto lugar, la aprobación de las guías de actuación para los sujetos obligados.

Reglamentariamente se prevé la posibilidad de crear comités dependientes de la Comisión. Atendemos al Comité de Inteligencia Financiera, que consiste en un nuevo órgano de apoyo que tiene por objetivos la difusión de principios de los informes de inteligencia financiera, la aprobación de directrices sobre inteligencia financiera, el auxilio al SEPBLAC con recomendaciones sobre el Plan Anual de Inspección de los sujetos obligados, la propuesta de medidas de mitigación de riesgos y la tarea de realizar estudios de tipologías. El director del SEPBLAC informa en las reuniones del Comité de Inteligencia Financiera de las tendencias en operativas sospechosas, la evolución del número y calidad de las comunicaciones y de la detección de patrones de riesgo de blanqueo de capitales y financiación del terrorismo.

La Ley 10/2010, de 28 de abril, establece como primer órgano de apoyo de la Comisión a la Secretaría, dependiente orgánica y funcionalmente de la primera. La Secretaría orienta las directrices de funcionamiento de la Comisión. Ejerce además las siguientes funciones: la adopción de acuerdos para la realización de actuaciones previas a la incoación de procedimientos sancionadores; la instrucción de los procedimientos sancionadores por infrac-

ciones previstas en la Ley 10/2010, de 28 de abril; la elevación al Comité Permanente de la Comisión de la propuesta de resolución de los procedimientos sancionadores a que hubiere lugar por la comisión de infracciones graves y muy graves previstas en la Ley 10/2010, de 28 de abril; y la coordinación de la participación española en los foros internacionales contra el blanqueo.

El SEPBLAC se trata del segundo órgano de apoyo de la Comisión. En punto a sus funciones, auxilia a los órganos administrativos y judiciales, al Ministerio Fiscal y a la Policía Judicial, analiza la información recibida y efectúa recomendaciones a los sujetos obligados para la mejora de las políticas de control interno. El SEPBLAC actúa con autonomía e independencia, sin perjuicio de directrices de la Comisión. Esto es, no recibe instrucciones de otro órgano para el análisis de casos, que se realiza conforme a criterios técnicos.

En su rol de inteligencia financiera, el SEPBLAC dispone de autoridad para decidir sobre la petición y la transmisión de información. Se erige como la entidad de control externo para la recepción de los informes de operaciones sospechosas, así como para la difusión de inteligencia financiera. Se establece al margen de las Fuerzas y Cuerpos de Seguridad del Estado o del Ministerio Fiscal. Es la principal herramienta para combatir el blanqueo de capitales vinculado al crimen organizado mediante la formación de inteligencia financiera, objeto de remisión posterior a las autoridades competentes.

## BIBLIOGRAFÍA

**Alcaraz Lamana, C.**, *La investigación de los delitos económicos y relacionados con la corrupción. Apuntes*. Tirant lo Blanch, Valencia, 2016.

**Álvarez Pastor, D., Eguidazu Palacios, F**., *Manual de prevención del blanqueo de capitales*. Marcial Pons, Madrid, 2007.

**Blasco Díaz, J. L.**, «Capítulo VII. La organización institucional», en Vidales Rodríguez, C. (dir.): *Régimen jurídico de la prevención y represión del blanqueo de capitales*. Tirant lo Blanch, Valencia, 2015.

**Carlos de Oliveira, A. C.**, «The Anti-Money Laundering Architecture of Spain», en Vogel B. y Maillart, J. (eds.): *National and International Anti-Money Laundering Law*. Intersentia, Cambridge, 2020.

**Carrillo del Teso, A. E.,** «Unidades de inteligencia financiera: las TICs en la prevención del blanqueo de capitales», en Pérez Álvarez, F. (ed.): *Moderno discurso penal y nuevas tecnologías: memorias [del] III Congreso Internacional de Jóvenes Investigadores en Ciencias Penales, 17, 18 y 19 de junio de 2013*. Ediciones Aquilafuente, Salamanca, 2014.

**De la Torre Lascano, M.,** *Lavado de activos: estudio sobre la prevención (en especial referencia al caso ecuatoriano)*. Tirant lo Blanch, Valencia, 2020.

**Deleanu, I., Van den Broek, M.**, «International cooperation», en VV. AA.: *The Economic and Legal Effectiveness of the European Union´s Anti-Money Laundering Policy*. Edward Elgar Publishing, Cheltenham, 2014.

**González Cussac, J. L., Larriba Hinojar, B.**, *Inteligencia económica y competitiva. Estrategias legales en las nuevas agendas de seguridad nacional*. Tirant lo Blanch, Valencia, 2012.

**González Cussac, J. L., Larriba Hinojar, B., Fernández Hernández, A.,** «Capítulo 19. Los servicios de inteligencia en el Derecho español», en González Cussac, J. L. (coord..): *Inteligencia*. Tirant lo Blanch, Valencia, 2012.

**González Cussac, J. L.,** «Inteligencia y Derecho», en Antón Mellón, J. (coord.): *Teoría de la Inteligencia en sistemas políticos democráticos*. Tirant lo Blanch, Valencia, 2024.

**Hava García, E.,** «Blanqueo de capitales», en Díaz Fernández, A. M. (dir.): *Conceptos fundamentales de inteligencia*. Tirant lo Blanch, Valencia, 2016.

**Jiménez García, F.,** *La prevención y lucha contra el blanqueo de capitales y la corrupción: Interacciones evolutivas en un derecho internacional global*. Comares, Granada, 2015.

**Jiménez Villalonga, R.,** «Capítulo IV. Tipos de inteligencia», en López Muñoz, J. (coord.): *Manual de Inteligencia. 2ª edición*. Tirant lo Blanch, Valencia, 2023.

**Llavador Piqueras, J., Llavador Cisternes, H.,** *El régimen jurídico de los servicios de inteligencia en España*. Tirant lo Blanch, Valencia, 2015.

**Mcdonell, R.**, «UN Anti-Money Laundering Initiatives», en Muller, W. H.; Kälin, C. H.; y Goldsworth, J. G. (eds.): *Anti-Money Laundering: International Law and Practice*. Wiley Editorial, Chichester, 2007.

**Muller, W. H.,** «The Egmont Group», en Muller, W. H.; Kälin, C. H.; y Goldsworth, J. G. (eds.): *Anti-Money Laundering: International Law and Practice*. Wiley Editorial, Chichester, 2007.

**Nieto Martín, A.**, «Transformaciones del Ius Puniendi en el derecho global», en Nieto Martín, A. y García Moreno, B. (dirs.): *Ius puniendi y global law: Hacia un derecho penal sin estado*. Tirant lo Blanch, Valencia, 2019.

**Pérez Marín, M. Á.,** «Las unidades de inteligencia financiera: el intercambio de información como medio para la prevención, la investigación y el enjuiciamiento de la delincuencia económica vinculada con el terrorismo», en Jimeno Bulnes, M. (dir.): *La evolución del espacio judicial europeo en materia civil y penal: su influencia en el proceso español*. Tirant lo Blanch, Valencia, 2022.

**Rodríguez Marcos, A. M.,** «Capítulo II. Seguridad e inteligencia», en López Muñoz, J. (coord.): *Manual de Inteligencia. 2ª edición*. Tirant lo Blanch, Valencia, 2023.

**Úbeda Martínez-Valera, P.,** *Obligaciones derivadas de la Ley de prevención del blanqueo de capitales en el ámbito de las profesiones jurídicas. Especial referencia al abogado*. J. M. Bosch, Barcelona, 2024.

**Urbaneja Cillán, J.,** «Acciones contra el blanqueo de capitales en el marco latinoamericano y caribeño», en *Anuario de la Facultad de Derecho de la Universidad de Extremadura*, n.º 29, 2011.

# EL PAPEL DEL SEPBLAC COMO UNIDAD DE INTELIGENCIA FINANCIERA EN LA LUCHA CONTRA EL FRAUDE FISCAL Y EL BLANQUEO DE CAPITALES

**Raquel Alamà Perales**
*Profesora e investigadora predoctoral (ACIF)*
*Universidad de Valencia*

## 1. Introducción

Es innegable que el delito de blanqueo de capitales es uno de los fenómenos que se ha consolidado como un enemigo del orden económico, político y social de primer orden a nivel mundial. Su alcance más allá de las fronteras nacionales, su conexión con delitos graves como el fraude fiscal, el narcotráfico o la financiación del terrorismo, así como el manejo de estructuras complejas y opacas que propician su carácter escurridizo ante el escrutinio de la legalidad, lo han erigido como una amenaza estructural de los sistemas financieros e incluso de la propia integridad del Estado de derecho. Desde finales del siglo XX, la comunidad internacional ha venido promulgando propuestas de cooperación internacional en aras de cimentar un marco normativo e institucional cada vez más sofisticado conforme las demandas sociales ante una criminalidad dinámica, tecnológica y cambiante[1].

En búsqueda de un binomio cuya fórmula aunase estándares globales de prevención y mecanismos de cooperación operativa entre Estados, el punto de inflexión lo marcó la Convención de Viena de 1988, al liberar el blanqueo de capitales del delito de narcotráfico[2]. Nacía un nuevo delito autónomo que sacudió los cimientos de la cooperación internacional adoptando un nuevo enfoque en el que los Estados se sometían a obligaciones de control y

1. Tondini, B., *Blanqueo de capitales y lavado de dinero: su concepto, historia y aspectos operativos,* Centro Argentino de Estudios Internacionales, 2006, vol. 38. págs. 2-10.

2. NACIONES UNIDAS, *Convención de las Naciones Unidas contra el Tráfico Ilícito de Estupefacientes y Sustancias Psicotrópicas*, Viena, 20 de diciembre de 1988, Naciones Unidas, Serie de Tratados, vol. 1582, pág. 95.

colaboración. El Grupo de Acción Financiera (GAFI) tan sólo tardó un año en seguir avanzando en este sentido, estableciendo las 40 Recomendaciones[3] que, sin saberlo, transformaron el derecho internacional en lo que hoy constituyen la referencia central de los sistemas de prevención a nivel mundial. A través de la Vigesimonovena Recomendación, el GAFI creaba las Unidades de Inteligencia Financiera (UIFs), lo que, paralelamente y en el plano operativo, el Grupo Egmont de UIFs, nacía en 1995 para configurar una red global que velara por el intercambio de información financiera, superando los obstáculos jurisdiccionales y el secreto bancario[4].

En España, las preocupaciones por el blanqueo de capitales llevaron a que el legislador incorporara plenamente esta arquitectura internacional en la Ley 10/2010, de prevención del blanqueo de capitales y de la financiación del terrorismo, y su Reglamento de desarrollo (RD 304/2014). A través de estas, se construía un marco normativo alineado con los estándares internacionales y se creaba oficialmente el Servicio Ejecutivo de la Comisión de Prevención del Blanqueo de Capitales e Infracciones Monetarias (SEPBLAC) como UIF española. En su constitución se optó por dotarla de naturaleza híbrida —con funciones de inteligencia y también de supervisión administrativa— lo que la convierte en un modelo singular dentro del derecho comparado y un actor fundamental en el ejercicio de las políticas de prevención de blanqueo de capitales[5].

En este sentido, la cooperación entre el SEPBLAC y la Agencia Estatal de Administración Tributaria (AEAT)[6] constituye uno de los pilares más relevantes del sistema español de prevención del blanqueo de capitales. Especialmente debido a que el fraude fiscal y el lavado de activos encuentran elementos comunes en su comisión —tales como la ocultación o el uso de entramados societarios complejos—, el binomio entre ambas instituciones genera sinergias de cooperación que permite un flujo bidireccional de información, gracias a la comunicación del SEPBLAC a la Administración Tributa-

3. Grupo de Acción Financiera Internacional (GAFI), *Las 40 Recomendaciones del GAFI*, París, 2012 (actualización de 2021).

4. Villavieja Urzinqui, L., «Análisis comparativo de los sistemas preventivos de lucha contra el blanqueo de capitales en Estados Unidos y en Europa», en *Relations*, 2007, pág. 221; Carrillo del Teso, A. E., «Unidades de inteligencia financiera: las TICs en la prevención del blanqueo de capitales», *Moderno discurso penal y nuevas tecnologías: memorias [del] III Congreso Internacional de Jóvenes Investigadores en Ciencias Penales, 17, 18 y 19 de junio de 2013*, Ediciones Universidad de Salamanca, 2014, págs. 188-193.

5. Pérez Marín, M. A., «La protección del sistema financiero en el ordenamiento español: el SEPBLAC como unidad de inteligencia financiera», *Derecho procesal: retos y transformaciones*. Atelier, 2021, págs. 495-497.

6. Al respecto, vid. Martínez Giner, L. A., Moreno González, S., Lampreave Marquez, P., «Intercambio de información y medidas fiscales de efecto equivalente», Jornada Preparatoria del Congreso de la EATLP. Doc. nº8/2014. *Revista Instituto de Estudios Fiscales*, págs. 1-27.

ria de indicios de infracciones fiscales que detecta durante sus análisis financieros, mientras que la AEAT remite al SEPBLAC operaciones o estructuras sospechosas de blanqueo de capitales descubiertas[7]. La importancia de este vínculo cooperativo radica en que la inteligencia tributaria es esencial para desvelar entramados de evasión fiscal y estructuras societarias opacas, que a menudo son la base del blanqueo trasnacional y del fraude fiscal internacional. Gracias a esta colaboración, la información tributaria logra integrarse en el ciclo de la inteligencia financiera, potenciando la capacidad de detección temprana como forma más eficaz de intervención, así como el éxito de intervenciones posteriores.

El presente trabajo tiene como objetivo el análisis de la etiología y evolución de las UIF en España, haciendo referencia al plano internacional a través de un recorrido histórico desde la Convención de Viena de 1988, los hitos introducidos por el GAFI y el nacimiento del Grupo Egmont, para examinar de forma general el modelo español del SEPBLAC: su naturaleza, sus funciones y el diseño de las UIF. Posteriormente, se hace hincapié en la cooperación con la Agencia Tributaria y cómo fruto de ésta, se han realizado aportes significativos en la resolución de casos tan relevantes como el Fórum Filatélico o CaixaBank. El estudio pretende mostrar cómo el SEPBLAC se inserta en la red global de inteligencia financiera y cuáles son sus actuaciones con la Administración Tributaria en el contexto actual de la globalización económica y transformación tecnológica del crimen.

# 2. El origen de las UIF en el contexto de internacional

## 2.1. La Convención de Viena de 1988 y el origen de la cooperación global en blanqueo de capitales

En materia de blanqueo de capitales, el punto de inflexión en el panorama internacional vino con la Convención de las Naciones Unidas contra el Tráfico Ilícito de Estupefacientes y Sustancias Psicotrópicas, adoptada en Viena el 20 de diciembre de 1988. Este tratado respondió a la preocupación cada vez más pronunciada de la comunidad internacional por el incremento del narcotráfico y sus efectos devastadores sobre la estabilidad económica y social de los Estados. Así pues, se trata de un hito jurídico trascendental que cambió el paradigma jurídico a nivel internacional, pues por primera vez se reconoció expresamente el blanqueo de capitales como delito autónomo, independiente del delito subyacente. En su artículo 3, apartado 1, b), los Estados parte se comprometieron a tipificar como delito la convención o transferencia de bienes a sabiendas de que procedían del tráfico ilícito de drogas, así como de

7. Bajo el amparo del artículo 46 de la Ley 10/2010 y de los arts. 93 y 94 de la Ley General Tributaria.

la ocultación o encubrimiento de la naturaleza, origen, localización o propiedad de dichos bienes[8].

Por subsiguiente, el blanqueo de capitales dejó de ser visto como una simple actividad accesoria y pasó a considerarse un ilícito de carácter autónomo, sujeto a persecución penal internacional. Junto a la criminalización, se introdujeron en el texto medidas patrimoniales innovadoras. Así lo muestra el artículo 5, el cual obliga a los Estados a establecer mecanismos de identificación, localización, embargo y decomiso de los bienes obtenidos directa o indirectamente del narcotráfico. Esa disposición fue pionera al poner en el ojo del huracán los responsables individuales y los flujos financieros, así como en la recuperación de activos ilícitos. Esto supuso allanar el camino al desarrollo posterior de las legislaciones domésticas sobre el decomiso ampliado y la recuperación de activos[9]. Otro punto esencial residió en que la Conversión incorporó un régimen reforzado de cooperación internacional, gracias a la previsión de mecanismos de extradición, asistencia judicial recíproca, ejecución transnacional de medidas cautelares y colaboración entre autoridades policiales y judiciales.

Con ello, se buscaba terminar con las fronteras jurisdiccionales que hasta el momento habían obstaculizado la persecución eficaz del narcotráfico y del blanqueo vinculado al mismo[10]. Sin embargo, las aspiraciones eran igualmente proporcionales al nivel de limitaciones estructurales que adolecía la Convención de Viena. Su alcance material estaba restringido al blanqueo de capitales vinculado al tráfico de drogas, dejando fuera otras formas de criminalidad económica igualmente relevantes y graves. Se cita a modo ilustrativo la corrupción o el fraude fiscal. No obstante, su impacto supuso un antes y un después: ya que los Estados quedaban obligados a tipificar el blanqueo dentro de sus códigos penales y, a su vez, debían adoptar medidas de cooperación financiera, en aras de impulsar a los Estados a crear estructuras nacionales especializadas[11]. Consecuentemente, años después, se consolidarían las UIF como entes independientes.

La doctrina coincide en señalar que la Convención de Viena inauguró la fase multilateral del régimen AML (*Anti Money Laundering*). Gracias a la transformación de un problema tratado hasta ese momento como una cuestión de índole doméstica, de repente, se convertía en un asunto de seguridad internacional. Por ende, no sólo hubo criminalización de conductas, sino que se

8. NACIONES UNIDAS, *Convención de las Naciones Unidas contra el Tráfico Ilícito..., op. cit.,* pág. 95., art. 3.

9. Vidales Rodríguez, C., «Blanqueo, ¿qué es blanqueo?, Vargas, A., Vargas Lozano. R. (dir.): *El Lavado de Activos y la Persecución de Bienes de Origen Ilícito*, Universidad Sergio Arboleda, Colombia, 2017, págs. 66-68.

10. INTERNATIONAL MONETARY FUND, *Financial Intelligence Units: An Overview*, Washington D.C., 2004, pág. 8.

11. Vidales Rodríguez, C., «Blanqueo, ¿qué es...?», *op. cit.*, págs. 69-72.

abrió la veda a la construcción de un sistema transnacional de prevención y represión, que sería posteriormente ampliado por el GAFI en 1989 con sus 40 Recomendaciones y consolidado operativamente con la creación del Grupo Egmont en 1995[12]. Consecuentemente, la Convención de Viena de 1988 se considera como la piedra angular del derecho internacional contra el blanqueo de capitales y, si bien no condiciona de forma directa el nacimiento de las UIFs, fue gracias a la aparición del delito de blanqueo como acción penal diferenciada del tráfico de drogas, lo que indirecta e inconscientemente creó el caldo de cultivo idóneo para la implementación de las Unidades de Inteligencia Financiera[13].

## 2.2. El GAFI y sus 40 Recomendaciones

El GAFI o Grupo de Acción Financiera Internacional —FATF, en inglés, o Financial Action Task Force— fue creado en 1989 en el marco de la Cumbre de G/ celebrada en París, como respuesta internacional a la creciente preocupación por el blanqueo de capitales vinculado al narcotráfico. Su primer mandato consistió en la elaboración de un conjunto de medidas de alcance global capaces de reforzar la integridad de los sistemas financieros de los países y ayudar a coordinar los esfuerzos nacionales contra el blanqueo de capitales. Lo que supuso considerar al lavado de activos como una forma de criminalidad transnacional. Apenas un año después de su constitución, el GAFI aprobó su primer paquete de propuestas, mundialmente conocido como las 40 Recomendaciones del GAFI; nacieron con el objetivo de consolidar un estándar para la lucha antiblanqueo.

Sin embargo, no constituyen un tratado internacional en sentido estricto, lo que las dota como soft law. Aun así, la influencia de las 40 Recomendaciones ha alcanzado las Directivas europeas, cristalizándose como derecho sustantivo y vinculante para los Estados —hard law—. Esto se debe, principalmente, al sistema de evaluación mutua (*mutual evaluations*) y a la presión internacional ejercida a través de instrumentos como las listas negras y grises del propio organismo[14]. Estas 40 Recomendaciones abordan aspectos fundamentales del sistema de prevención del blanqueo de capitales, así como su aspecto represivo. Entre ellas, se incluye la tipificación del delito de blanqueo de capitales como categoría autónoma de delito, la adopción de medidas de decomisación de activos de origen ilícito, embargo, imposición de obligaciones preventivas a los sujetos financieros —especialmente a ban-

12. Muller, W. H., The Egmont group. *Anti-Money laundering: International law and practice*, John Wiley & Sons. 2007, p. 83.

13. INTERNATIONAL MONETARY FUND, *Financial Intelligence Units: An Overview*, Washington D.C., 2004. págs. 1-3.

14. Daniels Pinto, A. L., ¿Qué es el GAFI y para qué sirve?, Acceso a la Justicia. Observatorio venezolano de la justicia. 2023, págs. 23-26.

cos y entidades de crédito—, la creación de UIF, el fortalecimiento de la cooperación internacional y la mejora de los mecanismos de asistencia judicial recíproca y extradición. En particular, la creación de las UIF se consagra en la Recomendación 29 como un pilar del sistema, pues exige que cada Estado disponga de una UIF capaz de recibir, analizar y difundir reportes de operaciones sospechosas presentadas por entidades obligadas[15] .

El GAFI ha revisado las 40 Recomendaciones en varias ocasiones con el fin de adaptarlas al trasiego incesante de la criminalidad económica. A destacar, la revisión llevada a cabo en 1996, amplió el blanqueo de capitales más allá del delito de narcotráfico hacia otros delitos graves; la de 2003, reforzó las medidas de diligencia debida del cliente e introdujo un mayor control sobre las Personas Políticamente Expuestas (PEP); la del 2012, incorporó una taxonomía de las disposiciones relativas a la financiación del terrorismo y la proliferación de armas de destrucción masiva, configurando un marco global que combate el blanqueo y el uso de los sistemas financieros con motivos terroristas[16].

Tal y como se ha hecho referencia previamente, el sistema de evaluación mutua es el mecanismo que mayor credibilidad le ha otorgado a las 40 Recomendaciones del GAFI; bien mediante la visita de expertos, bien a través del análisis detallado del riesgo, se consigue un alto grado de cumplimiento técnico de los estándares como la eficacia práctica de su implementación en cada Estado miembro. Los informes resultado de las inspecciones impactan profundamente en la reputación del Estado miembro, así como en la credibilidad de sus instituciones financieras. Los países señalados como no cooperadores enfrentan riesgo de ostracismo en los mercados internacionales y afrontan mayores dificultades para atraer capital extranjero[17]. Este efecto coercitivo ha transformado la premisa de considerar las 40 Recomendaciones como simple soft law, a establecerse como un verdadero soft law vinculante para los Estados miembros, gracias a su incorporación en las Directivas Europeas AML.

Actualmente, el GAFI cuenta con 39 miembros plenos y mantiene una red de organismos regionales, como el GAFILAT en América Latina o MONEYVAL[18]

---

15. Gluyas Millán, R., «Inteligencia financiera y prevención de lavado de dinero», en *ITER CRIMINIS Revista de Ciencias Penales*, núm 3. México 2006, pág. 45.

16. Den Broek, V., *The FATF and its Forty Recommendations: Global Standards against Money Laundering and Terrorist Financing*, Bruselas, 2019, pág. 112.

17. Daniels Pinto, A. L. ¿Qué es el GAFI...*?, op. cit.*, pág. 59.

18. Acrónimo de *Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism.* Se trata de un órgano especializado del Consejo de Europa, creado inicialmente en 1997 bajo el nombre de PC-R-EV (*Select Committee of Experts on the Evaluation of Anti-Money Laundering Measures*), para evaluar el cumplimiento de los Estados miembros en materia de lucha contra el blanqueo de capitales. MONEYVAL es fundamental porque garantiza la aplicación homogénea de las Recomendaciones del GAFI en Europa y regiones adyacentes, sirviendo de puente entre el Consejo de Europa y el sistema global de prevención.

en Europa. Estas estructuras aseguran la extensión de los estándares a más de 200 jurisdicciones en todo el mundo, lo que sitúa al GAFI en un verdadero legislador en materia de prevención del blanqueo y la financiación del terrorismo a nivel mundial[19].

## 2.3. El Grupo Egmont y la red mundial de UIF

En junio de 1995, veinticuatro representantes UIF se reunieron en el Palacio Egmont-Arenberg en Bruselas con el objetivo de crear un foro que permitiera superar las limitaciones propias del secreto bancario y las disparidades de la normativa doméstica, a través del establecimiento de un marco de cooperación que permitiese el intercambio de información financiera sensible en materia de blanqueo de capitales entre organismos homólogos. Esta primera reunión, considerada fundacional, dió lugar a la Declaración de Egmont, la cual sentó las bases de la actuación común de las UIF sobre los principios de confidencialidad, reciprocidad y flexibilidad institucional, así como el reconocimiento de la necesidad de crear canales tecnológicos seguros para el intercambio de información[20] Fue a partir de ese instante, que el denominado Grupo Egmont inició un proceso de consolidación institucional que evolucionó rápidamente hacia una estructura más compleja y organizada, con sede en Canadá[21].

En 1997, con motivo del pleno celebrado en Madrid se adoptó la Declaración de Principios del Grupo Egmont, que formalizó los procedimientos de adhesión de nuevos miembros y estableció criterios de funcionamiento interno, en aras de ser sujeta a revisiones sucesivas en La Haya (2001), Sídney (2003) y Guernsey (2004), con el objetivo de reforzar los estándares de admisión y garantizar un mayor control sobre la confidencialidad y dotar a la red de un mejor sentido organizativo[22]. Este escrutinio y sometimiento a revisión constante evidenció, a su vez, el crecimiento sostenido de la red, que comenzó a integrar UIF de distinta configuración y naturaleza jurídica, y grados diversos en cuanto a su desarrollo institucional.

El desarrollo normativo y operativo del Grupo Egmont se consolidó con la adopción de los *Principios Internacionales para el intercambio de información entre UIF*, aprobados en 2001 y revisados en 2013, que establecieron estándares mínimos de confidencialidad, reciprocidad entre UIF y restricciones en el uso de la información compartida, entre otros aspectos destacables[23]. Estos principios se consideran hoy un complemento añadido indis-

19. Den Broek, V., *The FATF and...», op. cit*., pág. 118,

20. INTERNATIONAL MONETARY FUND, *Financial Intelligence..., op. cit.,* pág. 102.

21. CANADÁ, *Global Affairs. Foreign Representatives in Canada: International Organizations and Other Offices*, Government of Canada, Ottawa, 2006.

22. INTERNATIONAL MONETARY FUND, *Financial Intelligence..., op. cit.,* pág. 103.

23. Blezzard, A., Koppe, H. V., *UIFs en Acción*. Grupo Egmont, 2000. p. 36.

pensable a la Recomendación 29 del GAFI[24], pues proporciona un marco operativo concreto para el intercambio de información financiera[25]. Junto a este hito, destaca la creación en 2010 de la ESW o la *Egmont Secure Web;* un sistema de comunicación cifrada que ha permitido institucionalizar un canal exclusivo para las UIF, asegurando no sólo la protección de datos especialmente sensibles, sino la agilización de la transmisión de datos en tiempo real durante investigaciones llevadas a cabo más allá de las fronteras nacionales y que revisten cierta complejidad, como aquellas relacionadas con grandes casos de corrupción, fraude fiscal internacional o financiación del terrorismo Más concretamente, destaca cómo el crecimiento del Grupo Egmont ha sido constante y principal en la arquitectura global en materia de prevención del blanqueo de capitales.

En 2019, la red alcanzó los 164 miembros; 167 en 2023. Esto supone la inclusión de prácticamente la totalidad de los Estados que cuentan con sistemas de prevención de lavado de activos y de la financiación del terrorismo consolidados[26]. El crecimiento exponencial ha contribuido a que la permanencia de un Estado en el grupo se considere como un sello de legitimidad internacional de carácter genuino. Esto supone que las UIF que no son miembros enfrentan graves obstáculos limitantes en cooperación con otras jurisdicciones y se exponen a evaluaciones negativas en los informes del GAFI y otros organismos internacionales. La admisión de nuevos integrantes está sometida a un escrutinio riguroso llevado a cabo por el Grupo de Trabajo Legal del Egmont, el cual desempeña un papel principal en la evaluación de las candidaturas. Para ello, se verifican que las UIF solicitantes cumplan con los estándares mínimos de independencia institucional, confidencialidad y capacidad operativa autónoma. Este protocolo procedimental busca evitar la entrada de Estados con sistemas precarios o deficientes que no aporten garantías suficientes de confidencialidad y que éstos se integren en la red. Consecuentemente, la credibilidad del grupo y la seguridad del sistema de intercambio de datos compartido por sus miembros se ven garantizados[27].

---

24. *«Los países deben establecer una Unidad de Inteligencia Financiera (UIF) que sirva como un centro nacional para la recepción y análisis de: (a) reportes de transacciones sospechosas; y (b) otra información relevante al lavado de activos, delitos determinantes asociados y el financiamiento del terrorismo, y para la comunicación de los resultados de ese análisis. La UIF debe ser capaz de obtener información adicional de los sujetos obligados, y debe tener acceso oportuno a la información financiera, administrativa y del orden público que requiera para desempeñar sus funciones apropiadamente».*

25. INTERNATIONAL MONETARY FUND, *Financial Intelligence..., op. cit.*, pág.74.

26. Fernández Liesa, C. R., «La prevención y lucha contra el blanqueo de capitales y la corrupción. Interacciones evolutivas en un Derecho internacional global.», en Revista Española de Derecho Internacional, vol. 67, núm. 2, 2015, pág. 308; Jiménez García, F., «Blanqueo de capitales y Derecho internacional», en *EUNOMÍA. Revista en Cultura de la Legalidad*, núm. 10, 2016, págs. 217-219.

27. INTERNATIONAL MONETARY FUND, *Financial Intelligence..., op. cit.,* pág.110.

Desde un punto de vista funcional, se desarrollan una amplia gama de actividades cuyo objetivo mayor consiste en la creación de UIF en países que carecen todavía de ellas, formar y asistir técnicamente a otras UIF en aras de fortalecer la capacidad operativa de las unidades menos desarrolladas, diseñar las tipologías de nuevas formas de blanqueo y financiación del terrorismo, y cooperar estrechamente con organismos internacionales como el GAFI, el FMI, el Banco Mundial o las Naciones Unidas. Así pues, no es solo un simple intercambio de pareceres, sino que se trata de un foro catalizador de estándares de buenas prácticas operativas. Por ende, se logra una homogeneización progresiva de los sistemas nacionales de inteligencia financiera. Sin embargo, y a pesar de que sus logros son patentes, el Grupo Egmont no está eximido de desafíos significativos. Su naturaleza jurídica no vinculante lo convierte en una institución catalogada de soft law, lo que se materializa en la dependencia de la voluntad política de los Estados miembros en última instancia para el éxito de sus medidas.

A su vez, concurren asimetrías notables en los recursos disponibles: mientras que los países desarrollados cuentan con tecnologías avanzadas de análisis masivo de datos gracias a la Inteligencia Artificial u otras herramientas fruto de digitalización o Cuarta Revolución Industrial —caso de FinCEN en Estados Unidos[28]—; otras UIF en países en desarrollo apenas cuentan con el personal y los recursos mínimos para el procesamiento de información recibida por los canales del Grupo Egmont. Esta disparidad de condiciones de base genera una desigualdad en el intercambio de información, poniendo en riesgo el principio de reciprocidad. Además, los conflictos normativos derivados de la fragmentación que acusan las jurisdicciones por las interpretaciones de cada Estado de la normativa internacional y que se plasma en cada derecho doméstico, supone la obstaculización de la plena cooperación incluso entre los miembros de la red en materias tan trascendentales como el secreto bancario o la protección de datos[29].

No obstante, el Grupo Egmont se ha consolidado como la columna vertebral de la cooperación operativa en inteligencia financiera. En palabras del propio FMI, la red complementa el marco normativo del GAFI con una infraestructura práctica de intercambio de información y coordinación que

28. El *Financial Crimes Enforcement Network* (FinCEN) es un organismo especializado del Departamento del Tesoro de los Estados Unidos, que actúa oficialmente como la Unidad de Inteligencia Financiera (UIF) estadounidense. Fue establecido el 25 de abril de 1990 mediante la Orden del Tesoro número 105-08, y su misión fue ampliada en mayo de 1994 para incluir responsabilidades regulatorias, consolidándose como una entidad clave en la arquitectura institucional de prevención del blanqueo de capitales. *Vid.* UNITED STATES GOVERNMENT. *Financial Crimes Enforcement Network (FinCEN).* Administra la ley de secreto bancario (Bank Secrecy Act – BSA) y una parte central de su operativa es la recepción de reportes de transacciones sospechosas (SARs – *Suspicious Activity Reports*). Disponible en: https://www.fincen.gov/

29. Blezzard, A., Koppe, H. V., *UIFs en..., op. cit.,* pág. 36.

permite convertir a las UIF en verdaderos nodos de una red transnacional de inteligencia financiera[30]. Gracias a ello, se ha erigido un mecanismo global capaz de hacer frente a las incógnitas referentes a fenómenos criminales de relevancia internacional como el blanqueo de capitales y la financiación del terrorismo.

## 2.4. Modelos comparados de UIF: administrativo, policial, judicial e híbrido

La literatura especializada coincide mayoritariamente en que, si bien todas las UIF comparten funciones nucleares consistentes en recibir, analizar y difundir la información susceptible de relevancia para la inteligencia financiera, el diseño orgánico de su anclaje institucional varía significativamente entre países. El carácter heterogéneo en su estructuración responde a trayectorias jurídicas e históricas distintas y a decisiones de política pública adoptadas durante la década de los noventa. La ausencia de un estándar internacional único consensuado conlleva a que, en la práctica, se distinguen cuatro tipologías de UIF: administrativa, policial, judicial —semejante a la fiscalía— e híbrida[31].

### 2.4.1. UIF administrativa

Dentro de la Administración, se alejan del marco orgánico de las autoridades policiales y judiciales. Operan como zona neutral entre los sujetos obligados y los órganos de investigación y persecución penal, lo que conlleva una reducción significativa de la fricción con la entidad policial cuando la fase de investigación es todavía temprana y no hay indicios plenos de delito. En algunos ordenamientos se adoptan en forma de agencia autónoma bajo supervisión ministerial; mientras que en otros, como entidad independiente con mandatos legales específicos. Entre sus ventajas están el fomento de la confianza del sector privado para el reporte, la coordinación interadministrativa y la capacidad para producir análisis estratégicos.

Entre sus límites, se señala la distancia operativa respecto de la investigación penal, pues se difiere en los plazos de respuesta, el acceso o en fuentes policiales reservadas. Así pues, este modelo prima la confianza de los bancos, lo que supone un incremento del número de reportes o beneficio, pero se pierde inmediatez en la persecución penal porque la UIF no tiene acceso

30. INTERNATIONAL MONETARY FUND, *Financial Intelligence..., op. cit.*, pág. 112. *«The Egmont Group has become the backbone of international FIU cooperation, complementing the FATF's normative framework with an operational network».*

31. INTERNATIONAL MONETARY FUND. *Establishing an FIU*. 2004, págs. 1-29. Disponible en: https://www.elibrary.imf.org/display/book/9781589063495/ch02.xml

directo a los datos policiales. Un ejemplo clásico de UIF administrativa en la comparación opera es la Oficina de Prevención del Blanqueo de Dinero de Eslovenia (OMLP), señalada como caso paradigmático[32].

### 2.4.2. UIF policial

Se integran dentro de los cuerpos y fuerzas de seguridad del Estado o de investigación criminal. Como puntos fuertes se destaca el acceso inmediato a bases de datos policiales, herramientas de investigación y cooperación operativa. Esto permite reducir el ciclo entre el análisis financiero y la apertura o impulso de las diligencias penales. Si bien, se suele apreciar alta reactividad ante amenazas de tipo emergente, lo que conlleva a la generación de reticencias en el sector privado a la hora de reportar por la proximidad directa a la coerción penal.

Caso paradigmático en la literatura comparada se cita la experiencia del Servicio Nacional de Inteligencia contra la Delincuencia (NCIS) del Reino Unido cuando ejerció funciones de UIF, siendo ejemplo del modelo judicial puro y sus *trade-offs*[33]. El modelo policial destaca por ganar rapidez para la conversión de la inteligencia en prueba, lo que permite la actuación inmediata. No obstante, la cantidad de reportes será menor porque los sujetos obligados pueden sentirse intimidados, lo que afecta sustancialmente al ejercicio comunicativo entre los sujetos obligados y las UIF[34].

### 2.4.3. UIF judicial

Este tipo de UIFs están adscritas al ministerio público o fiscalía, lo que determina su rasgo característico: la inmediatez en la judicialización de los casos. Al depender directamente de la fiscalía, las UIF disponen de un acceso privilegiado a medias procesales como el decomiso de bienes o el embargo de activos. Consecuentemente, se refuerza la cadena de custodia de la información financiera al convertirla en prueba judicial, lo que a su vez refuerza la calidad probatoria. Este modelo, no obstante, adopta una tendencia a centrarse exclusivamente en los aspectos penales, dejando en segundo plano el tan necesario análisis estratégico, así como las tareas de supervisión. La doctrina ha señalado que las UIF judiciales son más eficientes para asegurar la persecución penal, pero resultan menos versátiles como instrumentos de

32. INTERNATIONAL MONETARY FUND, *Financial Intelligence..., op. cit.*, págs. 10-14.

33. Literalmente significa compensación o contrapartida. Describe una situación en la que, al maximizar o ganar en un aspecto, necesariamente se pierde o se renuncia a otro. Es decir: un equilibrio entre costes y beneficios. En el contexto de las UIF (y de su diseño institucional), hablar de *trade-offs* implica reconocer que cada modelo (administrativo, policial, judicial o híbrido) ofrece ventajas, pero también sacrificios o costes asociados:

34. INTERNATIONAL MONETARY FUND, *Financial Intelligence..., op. cit.*, págs. 14-16.

política preventiva. A su vez, puede restringir la circulación de información hacia otros reguladores y, en algunos contextos, sobrecargar a la UIF con lógicas procesales que ralentizan el análisis estratégico[35].

### 2.4.4. UIF híbrida

Son aquellas UIF que combinan características de los modelos anteriores. Su diseño intenta buscar el equilibrio entre la confianza del sector privado —típica del modelo administrativo— con la capacidad operativa —típica de las UIF policiales y judiciales—. Estas de naturaleza mixta, suelen ser de carácter interinstitucional —caso de la participación de la Hacienda Pública, Interior, supervisores financieros, etc— y la operación con protocolos de derivación bien definidos en aras de reconducir, según el caso, la inteligencia hacía policía, fiscalía o reguladores administrativos. Según la literatura, el sistema híbrido supone una respuesta pragmática a los sistemas complejos, destacando la flexibilidad como punto positivo, pero alertado del reto que supone la gobernanza y coordinación en aras de evitar solapamientos, clarificar potestades y rendición de cuentas[36].

### 2.4.5. Consideraciones transversales de diseño

Más allá de la tipología de las UIF, hay una serie de factores o consideraciones transversales que resultan cruciales para el diseño institucional de cualquier UIF. En un primer acercamiento, la doctrina ha señalado que todas las UIFs, con independencia de su modelo, deben cumplir con un núcleo funcional mínimo. Es decir, deben ser capaces de operar con independencia y estar dotadas de los medios tecnológicos suficientes para recibir, analizar y difundir la información de relevancia para la inteligencia financiera. Estas tres acciones descritas son las que el Grupo Egmont y el GAFI reconocen como estándar mínimo internacional. Lo cual, sienta unas premisas sobre las cuales algunos Estados pueden añadir facultades adiciones, tales como la supervisión de sujetos obligados, la potestad de bloquear operaciones sospechosas de manera cautelar o la responsabilidad de impartir programas de formación y sensibilización en materia de prevención de blanqueo.

Sin embargo, este estándar hace de «suelo mínimo», lo que significa que no será admisible cualquier escenario en el que no se cumpla con los requisitos y no se supere dicho umbral. Asimismo, la ampliación de funciones, aunque son útiles para reforzar la eficacia preventiva, se deben ponderar cuidadosamente frente a las exigencias del principio de legalidad y del debido proceso, ya que suponen un desplazamiento de facultades tradicio-

35. INTERNATIONAL MONETARY FUND, *Financial Intelligence..., op. cit.*, pág. 16.

36 *Ibid.*, pág. 31.

nalmente atribuidas a autoridades judiciales o administrativas distintas[37]. Otro aspecto fundamental es dónde se integra la UIF o la ubicación institucional, así como la correlativa percepción de neutralidad. Eso se debe a que el anclaje administrativo favorece la confianza del sector privado y estimula el flujo de reportes de operaciones sospechosas, mientras que la UIF policiales y judiciales maximizan la capacidad de ejecución y la conexión con la persecución penal. Los modelos híbridos, por su parte, intentan mitigar los *trade-off*, si bien el precio de mayores costes de coordinación y riesgos de duplicidad de funciones[38].

La interoperabilidad internacional es otro factor transversal que resulta de gran relevancia. Si bien el carácter heterogéneo institucional no dificulta el reconocimiento mutuo dentro del Grupo Egmont, sí condiciona la calidad del intercambio. Es más, las UIF policiales y judiciales suelen priorizar la cooperación orientada a casos determinados y concretos, mientras que las administrativas tienden a compartir análisis estratégicos y alertas tipológicas. Las híbridas, pueden combinar ambas dimensiones, siempre y cuando en sus reglas de gobernanza, se encuentren claramente definidas para evitar solapamientos. Las opciones disponibles en materia de políticas públicas ofrecen un abanico de posibilidades a los Estados a la hora de crear o reformar sus UIF[39]: la ubicación orgánica más adecuada, la definición precisa de las funciones mínimas y accesorias, los mecanismos de supervisión y rendición de cuentas, los protocolos de intercambio de información y los perfiles profesionales del personal. El FMI subraya que la autonomía institucional, la claridad de mandato y la protección reforzada de la información son condiciones sine qua non para garantizar la eficacia de la unidad, independientemente del modelo elegido[40].

## 3. El Servicio Ejecutivo de la Comisión de Prevención del Blanqueo de Capitales e Infracciones Monetarias

En el caso español, la UIF es el Servicio Ejecutivo de la Comisión de Prevención del Blanqueo de Capitales e Infracciones Monetarias (SEPBLAC). Fue creado por mandato de la Ley 19/1993, de 28 de diciembre, sobre determinadas medidas de prevención del blanqueo de capitales, y se configuró como el órgano central de recepción, análisis y difusión de las comunicaciones de operaciones sospechosas precedentes de los sujetos obligados. Su naturaleza y funciones se desarrollan por la Ley 10/2010, de 28 de abril, de

37. INTERNATIONAL MONETARY FUND, *Financial Intelligence..., op. cit.*, pág. 33.

38. Gluyas Millán, R., «Inteligencia financiera...», *op. cit.,* pág. 61.

39. *Idem.*

40. INTERNATIONAL MONETARY FUND, *Establishing..., op. cit.,* págs. 3-27.

prevención del blanqueo de capitales y de la financiación del terrorismo, y por su Reglamento de desarrollo aprobado por Real Decreto 304/2014, de 5 de mayo[41].

## 3.1. Naturaleza y funciones

El SEPBLAC actúa como la UIF de España —art. 45.1 y 45.2 Ley 10/2010—, con una doble vertiente: por un lado, ejerce funciones de inteligencia financiera, en línea con los estándares del GAFI y pertenece al Grupo Egmont; de otro, despliega competencias supervisoras y sancionadoras sobre los sujetos obligados —arts. 44 y 45.2 de la Ley 10/2010; y art. 64 del Real Decreto 304/2014—, lo que lo convierte en una UIF híbrida. Se encuentra adscrita al Banco de España —art. 64 RD 304/2014—, pero actúa como órgano ejecutivo y permanente de la Comisión de Prevención del Blanqueo de Capitales e Infracciones Monetarias, presidida por el Secretario de Estado de Economía y Apoyo a la Empresa e integrada por representantes de diversos ministerios (Economía, Justicia, Interior, Hacienda) —art. 45.1 y 2 Ley 10/2010—, lo que le confiere una naturaleza híbrida, en tanto en cuanto se trata de una unidad administrativa dependiente de una autoridad monetario; a la vez que cumple funciones de coordinación con autoridades judiciales y policiales. Incluso fiscales. Esta dualidad refleja la neutralidad institucional exigida por los estándares internacionales y la eficacia operativa necesaria para la persecución penal.

A su vez, desarrolla una función de análisis estratégico, elaborando tipologías y evaluaciones de riesgo que se integran en la Estrategia Nacional contra el blanqueo y que sirven de guía tanto para las autoridades como para el sector privado[42]. A continuación, se desarrollan las más trascendentes:

### 3.1.1. Recepción, análisis y difusión de información financiera

El SEPBLAC recibe y analiza las comunicaciones de operaciones sospechosas (ROS) que los sujetos obligados deben remitir en virtud de los artículos 18 y 45.2 de la Ley 10/2010. Esta información constituye la materia prima de su función de inteligencia. A partir de ésta, se elaboran informes de inteligencia financiera en los que se identifican los patrones de riesgo, flujos sospechosos y posibles vínculos con delitos precedentes. Cuando se detectan indicios de blanqueo de capitales o financiación del terrorismo, se difun-

41. Ley 10/2010, de 28 de abril, de prevención del blanqueo de capitales y de la financiación del terrorismo, BOE n.º 103, 29 de abril de 2010 y Real Decreto 304/2014, de 5 de mayo, por el que se aprueba el Reglamento de la Ley 10/2010, BOE n.º 110, 6 de mayo de 2014.

42. Gluyas Millán, R., «Inteligencia financiera...», *op. cit.,* pág. 84.

den dichos informes a las autoridades competentes[43]. Entre los destinatarios habituales se encuentran las autoridades judiciales, las unidades de Policía Judicial —como la Unidad de Delincuencia Económica y Fiscal (UDEF) de la Policía Nacional o la Unidad Central Operativa (UCO) de la Guardia Civil—, así como las fiscalías especializadas, en particular la Fiscalía Anticorrupción y las secciones dedicadas a los delitos socioeconómicos. De esta manera, el SEPBLAC se configura como el eje de enlace entre el sector privado financiero y las instancias de persecución penal.

### 3.1.2. Supervisión de sujetos obligados

El SEPBLAC ostenta potestades de supervisión administrativa sobre los sujetos obligados, con el fin de garantizar el cumplimiento efectivo de las obligaciones preventivas previstas en la legislación. Esta función incluye el control de la correcta identificación de clientes o *know your customer* (KYC)[44], en aplicación de las medidas de diligencia debida —simplificada, normal o reforzada[45]—. A su vez, la obligación de conservar documentación durante al menos diez años[46], y la exigencia de establecer programas de formación interna para empleados[47].

Cuando el SEPBLAC detecta un incumplimiento, puede proponer la imposición de sanciones administrativas, formalmente acordadas por la Secretaría de Estado de Economía y Apoyo a la Empresa[48]. Consecuentemente, combina su papel de canal de inteligencia financiera, que conecta al sector privado con las autoridades represivas, con un perfil de supervisor administrativo que controla el cumplimiento normativo del sector financiero y de los profesionales sujetos a la ley. Este carácter híbrido lo convierte en un modelo singular dentro del marco comparado europeo.

### 3.1.3. Cooperación nacional e internacional

Una de las funciones esenciales del SEPBLAC es actuar como nodo de cooperación, tanto en el plano interno como en el internacional. En el ámbito nacional o doméstico, mantiene cauces de intercambio directo con la Policía Judicial y con la Fiscalía, conforme a lo previsto en los arts. 45.2 y 46 de la Ley 10/2010. Asimismo, coopera con la Agencia Estatal de Administración

43. Ley 10/2010, art. 46.

44. Ley 10/2010, arts. 3 a 6.

45. Ley 10/2010, arts. 7 a 10.

46. Ley 10/2010, art. 25.

47. Real Decreto 304/2014, de 5 de mayo, por el que se aprueba el Reglamento de la Ley 10/2010, BOE n.º 110, 6 de mayo de 2014, art. 29.

48. Ley 10/2010, arts. 50 a 52.

Tributaria (AEAT) en virtud de los artículos 93 y 94 de la Ley General Tributaria (LGT), que permiten el acceso a la información tributaria relevante para la prevención y represión del blanqueo de capitales. Estos mecanismos internos garantizan que la inteligencia financiera se integre en las investigaciones policiales, fiscales y tributarias, reforzando el carácter transversal de la lucha contra el blanqueo. En el caso del artículo 93 LGT, el SEPBLAC es un sujeto obligado al suministro de información constante a la AEAT, en aras de descubrir hechos susceptibles de interés tributario. No exclusivamente de la jurisdicción penal.

En el plano internacional, el SEPBLAC representa a España en la Red del Grupo Egmont, de la que forman parte más de 160 UIF de todo el mundo y a través de la cual se intercambian de forma segura comunicaciones de inteligencia financiera por medio de la Egmont Secure Web. Son precisamente estas comunicaciones las que permiten a los investigadores perseguir los flujos financieros a través de las distintas jurisdicciones en causas penales transnacionales de blanqueo de capitales y financiación del terrorismo o fraude fiscal, en los que se necesitan datos bancarios e historial de movimientos financieros procedentes de diversos países. Igualmente, el SEPBLAC colabora con otras agencias europeas como Europol, Eurojust y la Oficina Europea de Lucha contra el Fraude (OLAF), en operaciones conjuntas, investigaciones coordinadas, entre otras[49].

## 4. La cooperación del SEPBLAC con la Agencia Estatal de la Administración Tributaria

La Agencia Estatal de la Administración Tributaria (AEAT) desempeña un papel primordial en el sistema español de prevención del blanqueo de capitales, al constituir uno de los principales organismos de apoyo y colaboración con el SEPBLAC. No sólo en virtud el artículo 46 de la Ley 10/2010, éste está autorizado a comunicar información a otras autoridades nacionales competentes cuando en el ejercicio de sus funciones de análisis detecte indicios de infracciones tributarias, sino que en virtud el artículo 93 y 94 LGT, es un sujeto sometido a la obligación de intercambio de información con la AEAT. A su vez, la Administración Tributaria está facultada para hacer remisión al SEPBLAC de aquellas operaciones o estructuras financieras que puedan presentar indicios de blanqueo.

En lo que respecta al contenido tributario de los datos intercambiados con la UIF española, el marco normativo se complementa con lo dispuesto en el

49. La base legal de esta cooperación internacional se encuentra en el art. 46 de la Ley 10/2010, que autoriza la transmisión de información a UIF extranjeras y organismos internacionales competentes, así como en los arts. 65 y 66 del Real Decreto 304/2014, que regulan los protocolos y garantías de dicho intercambio.

artículo 95.1, apartados c) y d), de la Ley 58/2003, General Tributaria, que establece excepciones al carácter reservado de los datos tributarios, permitiendo su comunicación a las autoridades competentes cuando sea necesario para prevenir el blanqueo de capitales o para facilitar la investigación y persecución de delitos económicos. Esta previsión deviene imprescindible, pues se legitima el flujo de información tributaria de alta sensibilidad con las UIF, lo que en la práctica, deviene imprescindible para el rastreo de estructuras opacas y el análisis de esquemas de evasión fiscal. Elementos compartidos con el blanqueo de capitales, lo que convierte a la Hacienda Pública en una gran aliada de la UIF.

Asimismo, la AEAT se encuentra plenamente integrada en el SEPBLAC a través de su personal, conforme el convenio bilateral de 2006, en el que se acordó que la Administración Tributaria formaría parte de la propia Comisión de Prevención del Blanqueo de Capitales e Infracciones Monetarias, lo que cristaliza la coordinación institucional y participación activa en la definición de estrategias de prevención y represión del blanqueo de capitales y fraude fiscal. Este hito no es un mero formalismo fruto de las apariencias, pues durante la implementación de la amnistía fiscal de 2012, la AEAT remitió al SEPBLAC 705 reportes de contribuyentes con un perfil de riesgo especialmente significativo[50], sinónimo de ser sospechosos de comisión de blanqueo de capitales. Consecuentemente, se materializa el valor del flujo de información tributaria en el fortalecimiento de la inteligencia financiera[51]. Los datos estadísticos muestran que la magnitud de este binomio colaborativo no ha hecho más que aumentar; en 2018, la AEAT recibió 1327 informes del SEPBLAC y remitió 3 solicitudes formales. En 2022, estas cifras ascendieron a 1.757 informes recibidos y 11 peticiones atendidas[52], lo que evidencia un crecimiento sostenido del intercambio y la consolidación de este canal.

Casos de éxito que evidencian la fructífera colaboración entre el SEPBLAC y la AEAT, se ha visto reflejada en varios casos judiciales de gran repercusión mediática, lo que también permite analizar la integración de la inteligencia financiera en el proceso penal. En relación con el caso Fórum Filatélico, entre los años 2001 y 2003 el SEPBLAC detectó traspasos por más de 19 millones de euros procedentes de Gibraltar hacia empresas domiciliadas en España, con conexiones financieras hacia Suiza y Andorra[53]. Estas operaciones presentaban un claro componente transfronterizo, propio de las estructuras utilizadas para el lavado de capitales a través de paraísos fiscales y jurisdicciones opacas. La alerta temprana del SEPBLAC permitió trazar parte de los

50. RTVE, «La Agencia Tributaria sospecha de blanqueo de capitales en 705 acogidos a la amnistía fiscal», *RTVE Noticias*, Madrid, 17 de febrero de 2015.

51. Gluyas Millán, R., «Inteligencia financiera...», *op. cit.,* págs 59-88.

52. AGENCIA ESTATAL DE ADMINISTRACIÓN TRIBUTARIA, *Memoria de Actividades*, 2022.

53. *EL PAÍS*, «Economía investigó a Fórum en 2001 y 2003 por supuesto blanqueo de capitales», 16 de mayo de 2006.

flujos que, años después, serían investigados judicialmente en el marco del procedimiento penal contra Fórum Filatélico y Afinsa, conocidos por su utilización de un esquema piramidal encubierto bajo inversiones en sellos[i]. Este episodio muestra cómo la detección temprana de transferencias inusuales en circuitos financieros internacionales es esencial para activar la cooperación judicial y tributaria en varios Estados.

Por otro lado, la investigación abierta contra CaixaBank[54] constituye un caso relevante para comprender la función supervisora y sancionadora del SEPBLAC. La entidad fue investigada por haber permitido supuestamente la canalización sistemática de fondos de origen sospechoso mediante técnicas de *smurfing* (fraccionamiento de ingresos en múltiples operaciones de bajo importe para eludir los umbrales de control), en operaciones vinculadas sobre todo a redes criminales de origen asiático con presencia en España. El SEPBLAC, en su papel de autoridad de supervisión, había advertido de la deficiente aplicación de medidas de diligencia debida y de control interno, lo que condujo a la apertura de diligencias penales.

Ambos casos permiten poner de relieve el papel central del SEPBLAC como puente entre la información financiera y la persecución penal, ya sea a través de la detección temprana de movimientos internacionales —Fórum Filatélico— o mediante la supervisión directa del cumplimiento normativo en entidades financieras —CaixaBank—. Asimismo, prueban que el blanqueo de capitales en España no sólo consiste en la reinversión de capitales ilícitos dentro de las fronteras nacionales, sino que es fruto de esquemas internacionales que precisan de cooperación internacional constante, lo que supone desafíos estructurales derivados de la complejidad de las organizaciones criminales y de las posibles deficiencias en el control interno de las entidades financieras.

## 5. Conclusiones

La tendencia del régimen jurídico contra el blanqueo de capitales evidencia, desde una perspectiva internacional y doméstica, cómo este fenómeno ha dejado de ser una cuestión puramente interna para convertirse en un problema estructural de seguridad a nivel internacional. Desde la Convención de Viena de 1988, que supuso la declaración de independencia del delito de blanqueo del narcotráfico y la declaración de intenciones de la comunidad internacional en cooperar activamente hasta las 40 Recomendaciones del GAFI y la consolidación de la red del Grupo Edmonton, se ha establecido un marco operativo para las UIFs que brinda a los Estados miembros de las herramientas más sofisticadas para enfrentar los riesgos y consecuencias derivados de la criminalidad económica.

54. *EL PAÍS*, «La Audiencia Nacional imputa a CaixaBank por blanquear beneficios de mafias chinas», 19 de abril de 2018.

Ante estas circunstancias, el SEPBLAC ocupa un lugar protagonista en la arquitectura española de lucha y prevención del blanqueo de capitales. Su configuración como UIF híbrida, con atribuciones de inteligencia financiera y de supervisión administrativa, cumple un doble cometido: recibe y difunde información financiera estratégica, a la vez que controla y sanciona a los sujetos obligados. Es por tanto, muy versátil a la vez que complejo dentro del marco comparado europeo. En este sentido, la cooperación con la AEAT es un ejemplo paradigmático de cómo se integra la información tributaria y financiera en la trazabilidad de estructuras opacas, ampliamente utilizadas por delitos de fraude fiscal y blanqueo de capitales. Esto permite descubrir en un único proceder, indicios de fraude y blanqueo.

Los datos sobre el intercambio de información en los últimos y más recientes reportes de la autoridad tributaria muestran un aumento significativo en la colaboración, lo que refuerza la eficacia preventiva y represiva del sistema. Asimismo, los casos del Forum Filatélico y CaixaBank muestran en la práctica el impacto de la inteligencia financiera en la detección precoz de operaciones sospechosas y en la supervisión del cumplimiento normativo de las entidades financieras. Sin embargo, hay retos que afrontar: la asimetría de recursos y herramientas tecnológicas disponibles entre las UIF del Grupo Egmont; los problemas derivados de la fragmentación normativa, la duplicidad competencial en las UIF híbridas hacen patente la necesidad de refuerzo interno en cuanto a gobernanza y procesamiento masivo de datos, y una mayor coordinación a escala internacional.

## BIBLIOGRAFÍA

**Blezzard, A.**, **Koppe, H. V.**, *UIFs en Acción*. Grupo Egmont, 2000.

**Carrillo del Teso, A. E.**, «Unidades de inteligencia financiera: las TICs en la prevención del blanqueo de capitales», *Moderno discurso penal y nuevas tecnologías: memorias [del] III Congreso Internacional de Jóvenes Investigadores en Ciencias Penales, 17, 18 y 19 de junio de 2013*, Ediciones Universidad de Salamanca, 2014.

**CANADÁ**, *Global Affairs. Foreign Representatives in Canada: International Organizations and Other Offices*, Government of Canada, Ottawa, 2006.

**Daniels Pinto, A. L.**, ¿Qué es el GAFI y para qué sirve?, Acceso a la Justicia. Observatorio venezolano de la justicia. 2023.

**Den Broek, V.**, *The FATF and its Forty Recommendations: Global Standards against Money Laundering and Terrorist Financing*, Bruselas, 2019.

**Fernández Liesa, C. R.**, «La prevención y lucha contra el blanqueo de capitales y la corrupción. Interacciones evolutivas en un Derecho internacional global.», en Revista Española de Derecho Internacional, vol. 67, núm. 2, 2015.

**Gluyas Millán, R.**, «Inteligencia financiera y prevención de lavado de dinero», en *ITER CRIMINIS Revista de Ciencias Penales*, núm 3. México 2006.

**INTERNATIONAL MONETARY FUND**, *Financial Intelligence Units: An Overview*, Washington D.C., 2004.

**Jiménez García, F.**, «Blanqueo de capitales y Derecho internacional», en *EUNOMÍA. Revista en Cultura de la Legalidad*, núm. 10, 2016.

**Martínez Giner, L. A.**, **Moreno González, S.**, **Lampreave Marquez, P.**, «Intercambio de información y medidas fiscales de efecto equivalente», Jornada Preparatoria del Congreso de la EATLP. Doc. nº8/2014. *Revista Instituto de Estudios Fiscales.*

**Muller, W. H.**, The Egmont group. *Anti-Money laundering: International law and practice*, John Wiley & Sons. 2007.

**NACIONES UNIDAS**, *Convención de las Naciones Unidas contra el Tráfico Ilícito de Estupefacientes y Sustancias Psicotrópicas*, Viena, 20 de diciembre de 1988, Naciones Unidas, Serie de Tratados, vol. 1582.

**Pérez Marín, M. A.**, «La protección del sistema financiero en el ordenamiento español: el SEPBLAC como unidad de inteligencia financiera», *Derecho procesal: retos y transformaciones*. Atelier, 2021.

**Tondini, B.**, *Blanqueo de capitales y lavado de dinero: su concepto, historia y aspectos operativos,* Centro Argentino de Estudios Internacionales, 2006, vol. 38.

**Vidales Rodríguez, C.**, «Blanqueo, ¿qué es blanqueo?, Vargas, A., Vargas Lozano. R. (dir.): *El Lavado de Activos y la Persecución de Bienes de Origen Ilícito*, Universidad Sergio Arboleda, Colombia, 2017.

**Villavieja Urzinqui, L.**, «Análisis comparativo de los sistemas preventivos de lucha contra el blanqueo de capitales en Estados Unidos y en Europa», en *Relations*, 2007.

# EL IMPACTO DE LA INTELIGENCIA ARTIFICIAL Y LA AUTOMATIZACIÓN DE DATOS EN LA TOMA DE DECISIONES EN EL SECTOR PÚBLICO

**Blanca Aparicio Araque**
*Profesora e investigadora predoctoral (FPU)*
*Universidad de Castilla-La Mancha*

## 1. Introducción

Actualmente, la inteligencia artificial ha irrumpido en todos los sectores de la vida cotidiana, como pueden ser: la salud, la automoción, la robótica, la industria, la educación, etc., lo que se traduce en innumerables ventajas a la hora de promover una realización automática de múltiples tareas, lo que finalmente reporta un gran ahorro de tiempo, e incluso un menor desgaste del equipo humano que forma parte de las organizaciones.

El uso de estos sistemas inteligentes también se ha dejado entrever en el sector público, en concreto en el sector judicial o el sector de defensa. Respecto al sector judicial, entre los sistemas más utilizados destacan las herramientas de predicción de reiteración de riesgo delictiva, como la herramienta *Ris Canvi,* que permite predecir el riesgo de reiteración delictiva ajustándose a unos parámetros preestablecidos. De otro lado, en el sector de defensa o seguridad nacional, los sistemas de inteligencia artificial están permitiendo actualmente confeccionar armas de defensa, y de ataque, con un calibre que difícilmente podía imaginarse hace años. Estos sistemas permiten detectar la presencia humana a miles de kilómetros de distancia, así como la teledirección de equipos de forma remota, sin necesidad de que las personas físicas atacantes se encuentren en el objetivo determinado.

Pese a las innegables ventajas que reportan estos sistemas en la toma de decisiones del sector público, no podemos obviar los diferentes riesgos que se derivan del uso de estos dispositivos. Nos encontramos con herramientas que, aunque deben ser entrenadas en los *sadboxes* diseñados para ello, todavía no han encontrado su mejor versión, por lo que, en algunos aspectos, no se consideran la aliada perfecta. Si bien es cierto que, por ejemplo, en el caso de las decisiones judiciales automatizadas, pueden servir como orientación al

juzgador para una decisión final, si las convertimos en nuestro único punto de apoyo, podemos estar cometiendo un grave error. Esto se debe a que, en múltiples ocasiones, se ha podido corroborar que estas herramientas se encuentran sesgadas, por lo que, antes de dejarles el poder de tomar la decisión, debemos conocer si han sido alimentadas con datos suficientemente representativos. De otro lado, las características principales de estos sistemas, como son la baja trazabilidad y la falta de transparencia, son elementos que no ayudan a la comprensión de sus decisiones. Es por esto por lo que, aunque se puedan convertir en un gran apoyo, deberíamos ser cautos en su uso, y más en cuanto a automatización de decisiones en el sector público se refiere.

# 2. La inteligencia artificial

## 2.1. Concepto

En primer lugar, la RAE define la inteligencia artificial como *«la disciplina científica que se ocupa de crear programas informáticos que ejecutan operaciones comparables a las que realiza la mente humana, como el aprendizaje o el razonamiento lógico»*[1]. Si bien es cierto que no cuenta con una sola definición, dependiendo del enfoque que le quiera dar cada autor, algunos consideran que es un campo de la ciencia y la ingeniería que se ocupa de la comprensión, desde el punto de vista informático, de lo que se denomina comúnmente como «comportamiento inteligente», que también se ocupa de la creación de artefactos que exhiben este comportamiento[2].

De otro lado, se defiende que al hablar de inteligencia artificial nos referimos a «una especialidad que tienen o pueden tener algunos algoritmos»[3]. En opi-

1. En un sentido similar se pronuncia López Rincón, que la define como *«aquella disciplina científica enfocada en la replicación sintética del pensamiento y razonamiento humano a través de programación informática basada en algoritmos, siendo máquinas que piensan como humanos pues imitan su pensamiento»*, en López Rincón, D., «Robots y abogacía», en *Derecho de los Robots*, obra colectiva, director Moisés Barrio Andrés, Ed. Wolters Kluwer, Madrid, 2018, pág. 192.

2. Pino Diez, R., *Introducción a la inteligencia artificial: sistemas expertos, redes neuronales artificiales y computación evolutiva*, Universidad de Oviedo, servicio de publicaciones, 2002, págs. 5-8., citado en Navas Navarro, S. y otros, *Inteligencia artificial: tecnología y derecho,* Ed. Tirant lo Blanch, Valencia, 2017, pág. 24.

3. Portellano, P., «Inteligencia Artificial y responsabilidad por productos», en *Revista de Derecho Mercantil,* núm. 316/2020, Editorial Civitatis, S.A., 2020, pág. 4. En este mismo sentido se pronuncian en Berlanga de Jesus, A., «El camino desde la inteligencia artificial al Big Data», en *Revista de Estadística y Sociedad*, n. 68, 2016, págs. 9-11, citado en Cotino Hueso, L., *Derechos y garantías ante la inteligencia artificial y las decisiones automatizadas*, ed. Aranzadi, Navarra, 2022, pág. 54, en el que se refiere al algoritmo de la inteligencia artificial como *«un conjunto de reglas que, aplicadas sistemáticamente a unos datos de entrada apropiados, resuelven un problema en un número finito de pasos elementales».*

nión del Parlamento Europeo, la inteligencia artificial es «la habilidad de una máquina de presentar las mismas capacidades que los seres humanos, como el razonamiento, el aprendizaje, la creatividad y la capacidad de planear»[4]. En este mismo sentido se pronuncian algunos autores, entendiendo que la IA es una tecnología que tiene como objetivo crear sistemas capaces de realizar tareas que normalmente requerirían inteligencia humana. Consideran que, aunque algunas aplicaciones de IA puedan presentar comportamientos que parecen humanos, en general, la IA no imita completamente el comportamiento humano[5].

Además, véase la definición que ofrecen las Normas de IA de JAMS[6], entendiendo que la IA, en sentido amplio, «se trata de un sistema basado en una máquina capaz de realizar tareas que de otro modo requerirían cognición» (norma 1, e). Algunos autores han criticado esta definición, argumentando que esta definición tan amplia podría abarcar una gran variedad de sistemas basados en máquinas, lo que podría traducirse en una aplicación extensiva de las normas, de forma que incluso los sistemas informáticos básicos entrarían dentro de esta definición[7].

Hay autores que entienden que la inteligencia artificial se basa en el método probabilístico, según el cual las máquinas se orientan hacia lo que perciben como la realidad más probable[8]. O incluso entiende que la misma

4. Noticias Parlamento Europeo, ¿Qué es la inteligencia artificial y como se usa?, creado el 8 de septiembre de 2020 y actualizado el 26 de marzo de 2021 [En línea]. En este mismo sentido se pronuncian en otros escritos, entendiendo que el término inteligencia artificial se aplica a los sistemas que manifiestan un comportamiento inteligente, al ser capaces de analizar su entorno y pasar a la acción con cierto grado de autonomía para así alcanzar unos objetivos específicos, tal y como se desprende de la Comunicación de la Comisión al Parlamento europeo, al Consejo europeo, al Consejo, al Comité económico y social europeo y al Comité de las regiones. Bruselas 25.4.2018 COM [En línea] (2018). https://ec.europa.eu/transparency/regdoc/rep/1/2018/ ES/COM-2018-237-F1-ES-MAIN-PART-1.PDF. En este mismo sentido se pronuncia Jonathan Kaftzan, que define la inteligencia artificial como «la simulación de la inteligencia humana, incorporando razonamiento, percepción, solución de problemas y planificación», citado en Cornago Baratech J.F., «El papel de la inteligencia artificial en la defensa nacional», en *Inteligencia artificial y defensa. Nuevos horizonte*s, obra colectiva, ed. Aranzadi, Navarra, 2021, pág. 47.

5. Martín Rodriguez, G., «Nuevos horizontes en las políticas de la UE en materia de inteligencia artificial: hacia el Derecho Europeo de la IA», en *La atribución de una responsabilidad jurídico penal e internacional de la inteligencia artificial*, obra colectiva, directora Beatriz García Sánchez, coordinador Francisco Jiménez, García, Ed. Iustel, Madrid, 2023, pág. 380.

6. Las Reglas de IA de JAMS están destinadas a gobernar las disputas que involucren IA, y no proporcionan normas o guías sobre el uso de la IA en los arbitrajes, sino que son un conjunto de reglas diseñadas para «refinar y aclarar los procedimientos para los casos que involucran sistemas de IA».

7. Cláusula y Reglas de Disputas de Inteligencia Artificial (23 abril 2024), Diario LA LEY, 3 de octubre de 2024, pág. 2.

8. V. Franco, S., «Inteligencia artificial y Blockchain, el yin y el yan de la tecnología», citado en Barona Vilar, S., *Algoritmización del derecho y de la justicia: de la Inteligencia Artificial a la Smart Justice*, Ed. Tirant Lo Blanch, Valencia, 2021, pág. 94.

es una combinación de tecnologías que agrupa datos, algoritmos y capacidad informática[9].Otros entienden que el concepto de IA se refiere a sistemas inteligentes que pueden pensar y aprender, lo que ayuda al ser humano en la toma de decisiones[10]. Por último, hay autores que defienden que son máquinas que actúan como si fueran inteligentes, sin poder pensar autónomamente en realidad[11].

## 2.2. Características principales

Las principales características de la inteligencia artificial son las siguientes: autonomía, conectividad, apertura, complejidad, opacidad del proceso de toma de decisiones y dependencia de datos[12]. La autonomía se traduce en la posibilidad de que los productos y sistemas de IA operen o se manifiesten de modo autónomo, sin supervisión ni control humanos. La conectividad y la apertura a las nuevas tecnologías digitales pueden comprometer la seguridad de los productos al permitir su exposición a ciberamenazas o piratería informática. La complejidad se puede traducir en un riesgo, puesto que se deriva de la integración de los sistemas de IA con otros productos, componentes, piezas, dispositivos, etc., en la medida en que esta interacción con diversos elementos puede dar lugar a una desviación de su uso previsto o previsible. La opacidad del proceso de toma de decisiones de los productos y sistemas basados en IA y la capacidad de mejorar su propio rendimiento debido al aprendizaje a partir de la experiencia, hace más difícil la predicción y comprensión de su funcionamiento y comportamientos. La dependencia de los datos, la calidad, exactitud y adecuación de estos son fundamentales para que los sistemas y productos en cuestión de comporten según lo esperado[13].

Los principales retos que plantean estas características en su conjunto son los de determinar el origen y los responsables de los daños causados por un dispositivo o servicio operado por IA, así como el de establecer la causalidad, lo que constituye un problema para la determinación de la responsa-

9. Libro Blanco sobre la Inteligencia Artificial – un enfoque europeo orientado a la excelencia y la confianza, (COM (2020) 65 final), citado en Barona Vilar, S., ob. cit., pág. 95.

10. V. Cornago Baratech, J.F, ob. cit., pág. 47.

11. Ayllon García, J. D., «La inteligencia artificial como medio de difusión y control de la fake news», en *El derecho en la encrucijada tecnológica, Estudios sobre derechos fundamentales, nuevas tecnologías e inteligencia artificial*, obra colectiva, ed. Tirant Lo Blanch, Valencia, 2022, pág. 219.

12. Véase al respecto, Aragão Seia, C., «Inteligencia artificial: responsabilidad civil 3.0», en *El impacto de la era digital en el derecho*, obra colectiva, coordinador Quiroga Corti, M.P., director López Ulla, J.M., ed. Aranzadi, Pamplona, 2023, pág. 495.

13. Últ. ob. cit., pág. 496.

bilidad civil, según sus reglas tradicionales, así como la indemnización por daños causados[14].

## 2.3. Los datos y la inteligencia artificial

La importancia de los datos a la hora de desarrollar sistemas de inteligencia artificial es esencial, y tanto el sector doctrinal como el legislador son conscientes de ello. Tal y como afirman algunos autores, en los datos es donde radica la esencia de la inteligencia artificial, de forma que cuantos más datos maneje el sistema, más operacional será, pudiendo ofrecer conclusiones más acertadas[15].

Por tanto, se convierten en elementos esenciales: la obtención, el almacenamiento y la utilización de datos, de forma que debe realizarse correctamente. Preocupa a la doctrina la forma en la que se obtienen los datos. Esto se debe a que estos datos se convierten en el «alimento» de estas máquinas de juzgar y, sobre todo, especial mención merecen los datos de carácter personal, que contienen información íntima, y que, como consecuencia de una serie de operaciones, pueden ser utilizados de forma incorrecta o para una finalidad diferente a aquella que motivó su obtención[16].

En este sentido, es preciso mencionar la Ley Orgánica del Poder Judicial[17] (en adelante, LOPJ), que establece una diferencia relevante en relación con la obtención y el tratamiento de los datos personales en sede judicial. El artículo 236 bis de la LOPJ clasifica el tratamiento de datos personales atendiendo a la finalidad jurisdiccional o no jurisdiccional de los mismos. En este sentido, la recopilación de datos de la primera categoría se obtiene durante el desarrollo de la actividad jurisdiccional, conformando todos ellos el expediente judicial. La administración de justicia, como exige la Ley Orgánica de Protección de Datos Personales[18] deberá recopilar el consentimiento del titular respecto de los datos que solicita y utiliza. Ciertamente, existen excepciones a esta manifestación del consentimiento, de forma que no será necesaria si concurre alguna de las circunstancias que menciona el artículo 236 ter, apartado 3, de la LOPJ: «*cuando el titular afectado es parte de un proceso judicial, y facilita voluntariamente los datos al titular; o cuando es la propia autoridad judicial quien requiere la información».* Por tanto, todos los datos

14. Aragão Seia, C., ob. cit., pág. 497.

15. Pineros Polo, E., «El juez-robot y su encaje en la constitución española. La inteligencia artificial utilizada en el ámbito de la toma de decisiones por los tribunales», en *Estudios de Deusto*, Universidad de Deusto, vol. 72/1, enero-junio 2024, pág. 60

16. Ídem.

17. Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial. BOE núm. 17, de 2 de julio de 1985.

18. Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales. BOE núm. 294, de 6 de diciembre de 2018.

personales que constan en los ficheros judiciales deben ser obtenidos por una de las dos vías que menciona el precepto señalado anteriormente, para poder después utilizarse para alimentar a un sistema de inteligencia artificial que esté al servicio de la administración de justicia[19].

# 3. Regulación de la inteligencia artificial

La regulación de la inteligencia artificial viene impulsada por las directrices marcadas por la Resolución del Parlamento Europeo, de 3 de mayo de 2022 en la era digital[20], así como por lo reseñado en el Libro Blanco sobre inteligencia artificial, un enfoque europeo orientado a la excelencia y la confianza, de 19 de febrero de 2020[21]. De entre otros muchos pronunciamientos normativos, cabe destacar el conocido como «Reglamento de Inteligencia Artificial»[22], (en adelante, el Reglamento de IA) que pone el acento en el uso de sistemas de inteligencia artificial como pueden ser el educativo, el sanitario, el policial el judicial, e incorpora un abanico de obligaciones y estándares mínimos de garantía que deben cumplir los fabricantes de estos softwares, así como los operadores económicos prestadores que, situados en terceros estados de la Unión Europea, asuman tareas de distribución dentro del mercado comunitario[23].

## 3.1. El Reglamento de IA: sistemas de alto riesgo

Puesto que el conjunto de herramientas que han sido mencionadas en la introducción de este trabajo, y de las que hablaremos posteriormente, son clasificadas como «de alto riesgo», en el Reglamento de IA, destacaremos cuáles son las obligaciones para sus proveedores.

En primer lugar, un sistema será considerado del alto riesgo cuando esté destinado a ser utilizado como componente de seguridad de uno de los productos contemplados en el anexo II del Reglamento, y abarcan las tecnolo-

19. Pineros Polo, E., ob. cit., pág. 63.

20. Resolución del Parlamento Europeo, de 3 de mayo de 2022, sobre la inteligencia artificial en la era digital (2020/2266(INI))

21. Libro Blanco sobre la inteligencia artificial - un enfoque europeo orientado a la excelencia y la confianza, de 19 de febrero de 2020, COM (2020), 65 final.

22. Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, de 13 de junio de 2024, por el que se establecen normas armonizadas en materia de inteligencia artificial y por el que se modifican los Reglamentos (CE) nº 300/2008, (UE) nº 167/2013, (UE) nº 168/2013, (UE) 2018/858, (UE) 2018/1139 y (UE) 2019/2144 y las Directivas 2014/90/UE, (UE) 2016/797 y (UE) 2020/1828 (Reglamento de Inteligencia Artificial). DOUE núm. 1689, de 12 de julio de 2024.

23. Jiménez Cardona, M., «Aplicación de la inteligencia artificial en la toma de decisiones jurisdiccionales (España)», en *Revista Quaestio Iuris*, Rio de Janeiro, vol. 16, núm. 03, 2023, pág. 1614.

gías de IA empleadas en: infraestructuras críticas, que pueden poner en peligro la vida y la salud de los ciudadanos; formación educativa o profesional, que pueden determinar el acceso a la educación y a la carrera profesional de una persona; servicios públicos y privados esenciales; aplicación de las leyes, que pueden interferir de los derechos fundamentales de las personas, etc.[24].

Una de las principales obligaciones es la de cumplir con los requisitos referentes a la calidad de los conjuntos de datos utilizados. Deben utilizarse datos de alta calidad, suficientemente pertinentes y representativos, libres de errores y completos en vista de la finalidad del sistema, y estadísticamente adecuados en atención a lo establecido en el artículo 10, apartado 3, que indica lo siguiente: «*los conjuntos de datos de entrenamiento, validación y prueba serán pertinentes, suficientemente representativos y, en la mayor medida posible, carecerán de errores y estarán completos en vista de su finalidad prevista. Asimismo, tendrán las propiedades estadísticas adecuadas, por ejemplo, cuando proceda, en lo que respecta a las personas o los colectivos de personas en relación con los cuales está previsto que se utilice el sistema de IA de alto riesgo. Los conjuntos de datos podrán reunir esas características para cada conjunto de datos individualmente o para una combinación de estos».*

Además, se deberá implementar un registro de actividad que permita trazar los resultados del algoritmo y conservar toda la documentación técnica actualizada y archivos de registro. También se debería implementar un registro de actividad que permita trazar los resultados del algoritmo y conservar toda la documentación técnica del proceso, a fin de que pueda ser evaluada por las autoridades, conforme a los artículos 11 y 12. Es fundamental garantizar la transparencia algorítmica desde el diseño y la comunicación de información a los usuarios, como establece el artículo 1.3. Se requiere también la supervisión humana de las decisiones automatizadas, de acuerdo con el artículo 14. Finalmente, se debe asegurar la precisión, solidez y ciberseguridad del sistema, como se indica en el artículo 15[25].

## 3.2. Las propuestas del Grupo de Trabajo del CGPJ sobre tecnología, inteligencia artificial y justicia

Debido a los fenómenos de digitalización, robotización y algoritmización de la Justicia, el Consejo General del Poder Judicial ha centrado sus esfuerzos en elaborar, desde mediados del año 2022, y mediante un Grupo de Expertos,

24. Reyes López, M. J., «La protección al consumidor al hilo de las nuevas propuestas legislativas comunitarias», en *Actualidad Civil*, núm. 7, editorial LA LEY, julio de 2023, pág. 4.

25. Todas estas obligaciones se detallen expresamente en Alkorta Idiakez, I., «La discriminación algorítmica en el sector sanitario», en *Inteligencia artificial y derecho de daños: cuestiones actuales. Acorde al Reglamento (UE) 2024/1689*, obra colectiva, coordinadores Juan A. Moreno Martínez, Pedro J. Femenía López, ed. Dykinson, Madrid, 2024, pág. 4.

un documento de Propuesta vinculado con la aplicación de la tecnología, la inteligencia artificial y la administración de justicia[26].

De estas propuestas, caben destacar las siguientes recomendaciones: uso prudente de aplicaciones de gestión procesal que automaticen diferentes actuaciones administrativas que no impliquen interacción con la ciudadanía y que proporcionen un conjunto elemental de datos a los procesos judiciales basados en el expediente electrónico; precauciones planteadas al hilo de la ciberseguridad certificable a nivel ISO; implementación de procedimientos de verificación de la calidad de sistemas de IA; creación de una Agencia sobre IA; diligencias debidas acercas del pre-proceso, incluyendo anonimización de datos de entrada, normalización documental, o unificación de sistemas; protección de datos personales, debiendo apostar por una IA confiable que contribuya a la anonimización y la pseudoanonimización, así como la incorporación de algoritmos guardianes; la aplicación de los principios de información previa, transparencia, confidencialidad, integridad y trazabilidad, la minimización en la conservación de datos, el reforzamiento tecnológico que permita la disociación de datos personales; la incorporación de previsiones relativas a los derechos de acceso, rectificación, opresión oposición y limitación; y todo ello unido al derecho a no ser objeto de una decisión basada únicamente en tratamientos automatizados[27].

En materia de decisiones automatizadas en el sector judicial, son especialmente reseñables las siguientes recomendaciones: las consideraciones relativas a la automatización de la tramitación, que incluyen la implementación progresiva, información sobre el estado procesal de un procedimiento, sistemas de avisos, digitalización del sistema de notificaciones y unificación de los mecanismos de consulta utilizables[28]. Por último, en relación con la toma de decisiones jurisdiccionales distingue cuatro grandes modelos de aplicación de la inteligencia artificial en la toma de decisiones jurisdiccionales, como son: asistencial o instrumental, cautelar, de ayuda a la decisión automatizada y justicia robotizada, en las que nos centramos en el apartado siguiente.

# 4. El impacto de la inteligencia artificial en las decisiones automatizadas

## 4.1. El impacto en el sector judicial

Tal y como destaca la doctrina, mediante algoritmos de inteligencia artificial es posible asistir decisiones judiciales con un elevado nivel de precisión,

26. Jiménez Cardona, M., ob. cit., pág. 1616.

27. Últ. ob. cit., pág. 1617.

28. Ídem.

en algunas ocasiones[29]. Respecto a las ventajas, destacan una mayor eficacia, teniendo en cuenta el crecimiento exponencial de litigios, unido al colapso actual de los juzgados a nivel nacional, por lo que estas herramientas podrían convertirse en grandes aliadas de los jueces, siempre y cuando se realizase un uso diligente de las mismas. Dentro de las funciones de este tipo de sistemas se encuentran la capacidad de evaluar pruebas, generar documentación, así como transcribir las vistas a través de reconocimiento de voz[30]. También se destacan de entre estas facultades el reconocimiento de textos e imágenes, lo que facilita la generación de documentación; así como la posibilidad de acumular muchos más datos de lo que podría acumular el propio ser humano, a la hora de revisar hechos y compararlos con casos previos incorporados a una base de datos. E incluso algunos autores advierten que el uso de este tipo de sistemas podría traducirse en la posibilidad de eliminar ciertas inconsistencias y la posible falta de neutralidad de los jueces humanos[31].

De otro lado, también se prevén una serie de limitaciones que ponen en tela de juicio el uso de estos sistemas en el ámbito judicial. Destaca la doctrina que, aunque la inteligencia artificial pueda ser ampliamente eficaz, la calidad de sus decisiones para valorar aspectos muy específicos de un caso no puede compararse con la de un juez. Además, estos sistemas suelen llevar aparejados una serie de limitaciones y sesgos, que pueden corresponder a errores de programación, incapacidad para valorar aspectos sutiles o sesgos conscientes o inconscientes introducidos en la programación por los desarrolladores[32].

Respecto a los sesgos, hemos de definirlos como «la orientación o dirección que toma un asunto, en este caso, los diferentes datos que se introduzcan». Hay diferentes tipos, clasificándose en sesgos conscientes e inconscientes. Los que más riesgos conllevan son estos segundos, pues son aquellos que se producen sin que la persona responsable del algoritmo tenga intención de introducirlos, debido a una falta de rigurosidad en la captación de los datos o el desconocimiento de cómo determinados datos pueden afectar a un resultado final[33]. A su vez, estos últimos admiten una subclasificación. De un lado, aquellos relativos al contexto cultural, geográfico y temporal, como el sesgo en la muestra que se produce cuando los datos recopilados no representan con precisión el entorno en el que se espera que se ejecute el programa; o el

29. Espinosa, P., Clemente, M., «La percepción de la toma de decisiones a través de inteligencia artificial cuando se produce daño a las personas», en *Estudios Penales y Criminológicos,* obra colectiva, Universidad de Santiago de Compostela, núm. 44, 2023, pág. 8.

30. Ídem. En China, esto ha supuesto una reducción de entre el 20 y el 30 % de la duración de los juicios, y hasta una reducción del 50 % en los juicios más complejos.

31. Idem.

32. Ídem.

33. Salazar García, I., «Retos actuales de la ética en la inteligencia artificial», en *Derechos y garantías ante la inteligencia artificial y las decisiones automatizadas*, obra colectiva, director Lorenzo Cotino Hueso, ed. Aranzadi, Navarra, 2022, pág. 60.

sesgo de exclusión, que se produce cuando se eliminan algunas características pensando que son irrelevantes para las etiquetas, teniendo en cuenta solo creencias existentes[34].

En segundo lugar, aquellos relativos al perfil de la persona que desarrolla el algoritmo, como es el sesgo del auditor de datos, que a la hora de analizar los datos ya sea el investigador o la persona que los audita, llegan a ellos con prejuicios abordándolos desde un punto de vista que concluye con una análisis sesgado; o los sesgos de perjuicios, que se producen cuando el desarrollador del algoritmo se deja influir de manera inconsciente por sus prejuicios personales, juzgando por la apariencia, la condición física, el género, etc.[35]. Por último, los sesgos en la medición y recogida de datos, de forma que en ocasiones el sesgo se produce en la recogida de datos, en función del instrumento con el que se recojan, como por ejemplo cuando se realiza a través de una cámara fotográfica con poca luminosidad[36].

Junto a la presencia de sesgos, hemos de añadir que los algoritmos suelen ser opacos, por lo que no hay una comprensión clara de cuál es el proceso que ha seguido para tomar una determinada decisión. Además, también se destaca que este tipo de sistemas no deberían nunca sustituir a la figura del juez puesto que no cuentan con la intuición, la percepción de las necesidades de las partes o el «saber hacer» que permite la experiencia de los jueces humanos[37].

### 4.1.1. Aplicación asistencial o instrumental

Respecto a la aplicación asistencial o instrumental de la inteligencia artificial en la toma de decisiones jurisdiccionales, es especialmente útil en relación con la potenciación y estandarización de formularios procedimentales, la argumentación jurídica que pueda derivar de la estadística descriptiva, el análisis de porcentajes y el estudio de la doctrina y la jurisprudencia que puedan resultar aplicables al caso concreto. En este sentido, es muy ilustrativo el ejemplo de la herramienta WATSON, que permite obtener en poco tiempo un listado de argumentos a favor y en contra de una determinada cuestión jurídica teniendo en cuenta el cribaje jurisprudencial[38].

De entre todo el elenco de sistemas que aparecen, se pone el acento en la evaluación de la solidez de los diferentes modelos de prueba, los asistentes fundados en la predicción y evaluación de riesgos, como el sistema *RISCANVI*, mencionado anteriormente, que se utiliza en los centros penitencia-

34. Ídem.

35. Ídem.

36. Ídem.

37. Espinosa, P., Clemente, M., ob. cit., pág. 8.

38. Jiménez Cardona, M., ob. cit., pág. 1617.

rios catalanes para medir, mediante un algoritmo, el riesgo de reincidencia de los reclusos y ayudar a las autoridades a tomar decisiones sobre su salida de prisión, así como para ponderar el riesgo de quebrantamiento de condena, la violencia intrainstitucional y la violencia dirigida. De otro lado, también destacan aquellas utilizadas para asistir al juez, en ámbito de segunda instancia, en aras a suministrarle una propuesta de estimación o desestimación en función de la adaptación de los motivos del recurso a la jurisprudencia consolidada sobre la materia. Como ejemplo, en este último caso destaca la herramienta BIDARACIV, a través de la cual se enfrenta la extracción automatizada de peticiones, decisiones, y argumentos en sentencias de custodia en los casos de divorcio[39].

### 4.1.2. Aplicación cautelar

Al estar contemplada esta aplicación por el Grupo de Trabajo del CGPJ, también debemos hablar sobre la utilización instrumental de la inteligencia artificial en el ámbito cautelar. De esta manera, se prevén ciertas herramientas de inteligencia artificial que pueden medir eL análisis de impacto y probabilidad de una medida cautelar en función de la determinación de los niveles de riesgo mediante la fijación de parámetros relativos al *fumus boni iuris*, el *periculum in mora* o incluso la fijación, en su caso, de la correspondiente caución[40].

En este sentido, la función principal de este tipo de sistemas es medir los riesgos de impago, la insolvencia o pérdida de la cosa, la estimación de prolongación temporal del proceso, la fijación de la cuantía de fianza, la concreción de la indemnización, el riesgo de fuga, etc., todo ello en atención a las circunstancias individuales de cada reo, teniendo en cuenta la naturaleza del hecho enjuiciable, la gravedad de la pena, la constatación de delitos conexos, la existencia de órdenes de busca, entre otras circunstancias personales[41].

La aplicación de todos estos criterios se puede extender también a la toma de decisiones relativas a acordar o no la libertad condicional de una persona, o los permisos y beneficios de los que se pueda llegar a beneficiar. Otros ejemplos son el sistema *COMPAS*, utilizado en EEUU para valorar el riesgo de reiteración delictiva, así como VIOGEN, como sistema de vigilancia integral en los casos de violencia de género contra la mujer que es capaz de predecir el riesgo de cada individuo implicado en un posible caso de violencia machista, así como el peligro colateral y las medidas de protección que los menores afectados puedan requerir en el caso concreto[42].

39. Últ. ob. cit., pág. 1617, 1618.

40. Últ. ob. cit., pág. 1618.

41. Últ. ob. cit., págs. 1618, 1619.

42. Últ. ob. cit., pág. 1619.

### 4.1.3. Aplicación de ayuda a la decisión automatizada

El Grupo de Trabajo del CGPJ propone la utilización del «juez robot», en aplicación sencilla de la ley reforzada por la aplicación de la jurisprudencia y las máximas de la experiencia, pero sometidos al control, por vía de recurso, ante el juez humano, la potenciación de la resolución de los litigios *on line* mediante formularios preordenados y con asignación aleatoria a organismos plurales de resolución de conflictos, los alimentos, las conformidades, los juicios rápidos, etc. Todo ello unido a la previsión de decisiones judiciales automatizadas por diseño sobre la base de la tecnología de registro distribuido, como es el caso de los *smart contracts*, *smart orders* e incluso de los metaversos[43].

### 4.1.4. Aplicación de justicia robotizada

En relación con el último escalón de desarrollo de la aplicación de la inteligencia artificial que contempla el Grupo de Trabajo del CGPJ en la toma de decisiones jurisdiccionales es la figura del Juez-Robot. Esta figura incorporaría tres modelos, en su dimensión genérica: (i) *el juez doctrinal*, que partiendo de la base de datos del CENDOJ reúne técnicas de aprendizaje automáticas y árbol de búsqueda, a su vez combinadas con una formación en casos prácticos reales derivados de una recopilación de datos de los servicios de gestión procesal de las diferentes Comunidades Autónomas, teniendo como ejemplo *AlphaJudge*; (ii) *el juez IA-normativo*, capaz de aprender en función de la legislación aplicable y que deberá comprender una fase de codificación legal apta para el lenguaje de programación, así como una segunda vinculada con el entrenamiento en redes neuronales mediante casos prácticos de resolución pacífica, teniendo como ejemplo *AlphaJudge Zero*; y (iii) *el juez IA-máximas de experiencias*, que deberá aprender de la experiencia resultante de los asuntos que se le plantean al alimentarse de datos sobre asuntos de primera y segunda instancia, así como la jurisprudencia del Tribunal Supremo[44].

Ahora bien, parte de la doctrina se muestra un tanto reticente a esta figura del «juez robot». Ello se debe a que entienden que los jueces son absolutamente soberanos en el ejercicio de la función jurisdicción, de forma que cuando ejercen su potestad deben estar sometidos única y exclusivamente a la ley, y no deben ser perturbados en el ejercicio de su cometido. Además, destacan las garantías legales de la independencia judicial, como es la inamovilidad judicial, de forma que nuestra Constitución establece la imposibilidad de separar, suspender, trasladar un jubilar a un miembro de la Judicatura, salvo por las causas previstas expresamente en la ley. Una vez explicado

43. Últ. ob. cit., pág. 1620.

44. Últ. ob. cit., págs. 1620, 1621.

esto, la doctrina se plantea si se podría predicar la actividad jurisdiccional que realicen las máquinas de juzgar[45].

Dentro de los principales argumentos que sostienen se encuentra la imposibilidad de extender la necesaria independencia a los humanos que crean el sistema de IA que realizará la actividad judicial. Entienden que esta tecnología está siendo desarrollada por empresas privadas, que desempeñan una actividad con opacidad, y cuyo producto está protegido por los derechos de autor. Las compañías privadas se rigen por sus criterios propios de organización y dependencia, de forma que no antepondrán el interés público al propio de carácter totalmente privado[46]. En este caso resulta de especial trascendencia es caso BOSCO. En 2018, Civio[47] solicitó el código fuente, las funcionalidades y los casos de prueba de BOSCO, el programa que decidía quién podía acceder al bono social eléctrico. La administración rechazó conceder ese acceso. Tras reclamar ante el Consejo de Transparencia y Buen Gobierno, se pudieron conocer las funcionalidades y los casos de prueba. Estos dos elementos permitieron demostrar que BOSCO había sido diseñado con errores que dejaban fuera a personas con derecho a la ayuda. Sin embargo, el Consejo de Transparencia también negó el acceso al código fuente, donde se detallaban todas las instrucciones del algoritmo, y con el que se hubiera podido confirmar o descartar la existencia de más errores. Amparándose en la propiedad intelectual y la seguridad, los tribunales desestimaron las peticiones respectivas en 2022 y 2024. En diciembre de 2024, el Tribunal Supremo admitió el recurso de casación por parte de esta fundación[48].

### 4.1.5. La digitalización de la justicia en América Latina

Como hemos indicado anteriormente, en España ya se han implementado algunos sistemas de inteligencia artificial dentro de nuestro sistema judicial. No obstante, hay algunos tipos de sistemas que son meras posibilidades, intangibles, al no haberse desarrollado todavía. Por tanto, hemos de analizar si todos estos sistemas se han implementado en países vecinos, y cuál ha sido su efectividad. *Fiscal Watson*, de Colombia, es un programa que incorpora semántica de datos para explorar la información contenida en las bases de datos de 13 millones de denuncias de todo el país para analizar similitudes

45. Pineros Polo, E., ob. cit., pág. 69.

46. Últ. ob. cit., pág. 70.

47. Fundación ciudadana española, independiente y sin ánimo de lucro, que se dedica a promover la transparencia y la rendición de cuentas de las instituciones públicas.

48. La transparencia de los algoritmos públicos, en juego: Civio presenta el recurso sobre BOSCO ante el Tribunal Supremo, de 30 de enero de 2025. Consultado en: https://civio.es/novedades/2025/01/30/la-transparencia-de-los-algoritmos-publicos-en-juego-civio-presenta-el-recurso-sobre-bosco-ante-el-tribunal-supremo/. Última fecha de consulta: 9 de julio de 2025.

y disociar casos, permitiendo también acceder en tiempo real a toda la información de criminalidad, las zonas de conflicto y georreferenciar los delitos[49]. Otro ejemplo es *E-Proc,* que es el primer sistema de procesamiento electrónico de la Justicia Federal de Brasil, y fue diseñado para combatir la lentitud procesal y permite la formalización práctica de actos procesales y el procesamiento y la gestión de procesos, documentos y procedimientos administrativos por medios digitales[50].

De otro lado, en Colombia la Fiscalía General de la Nación viene impulsando desde 2016 un sistema de inteligencia artificial para determinar el riesgo de reincidencia que representa un procesado y a través de ello poder definir, de forma racional y objetiva, si se debe solicitar prisión preventiva o cualquier otra medida de aseguramiento. Un ejemplo de ello es *PRISMA* (Perfil de Riesgo de Reincidencia para Solicitud de Medidas de Aseguramiento) que procesa datos obtenidos de la Policía Nacional, la Fiscalía y del Instituto Penitenciario y Carcelario de Colombia, lo que se traduce en casi seis millones de individuos con antecedentes, que permitirán predecir patrones de comportamiento asociados a los eventos delictivos y registros en un período de dos años posterior a la imputación. También destaca *VICTOR,* que es un sistema que elige de entre miles de recursos de apelación que recibe el Tribunal Supremo Federal de Brasil, aquellos que, por su repercusión o impacto social, merecen ser estudiados en profundidad. Así como la herramienta *Prometea*, desarrollada en Argentina con el objetivo de la agilización de los procesos judiciales en beneficio del ciudadano. Se probó en el dominio de amparos habitacionales, y su uso se extendió a casos de bonificaciones de empleo público, ejecución de multas no pagadas, negación de licencias de taxi por antecedentes penales y denuncias por violencia de género, entre otros. Lo que resulta ampliamente interesante es que *Prometea* ofrece un algoritmo de predicción sin «caja negra», de forma que el software que elabora dictámenes jurídicos, basándose en casos análogos, para cuya solución existen precedentes judiciales reiterados, añadiendo que todos los algoritmos que utiliza son trazables, de forma que existe una forma técnica para rastrear paso a paso cómo alcanzó un resultado determinado, evitando la configuración de cajas negras[51].

## 4.2. El impacto en el sector defensa

En primer lugar, debemos destacar que la inteligencia artificial se ha convertido, desde hace años, en una verdadera aliada en materia de seguridad, pues posibilita la obtención de grandes resultados en un menor tiempo y

49. De Lara- García, J., «Inteligencia Artificial y Judicial: Experiencias en América Latina», en *DIVULGARE, Boletín Científico de la Escuela Superior de Actopan*, Publicación semestral, vol. 9, núm. 17, 2022, pág. 44.

50. Ídem.

51. Ídem.

con menos esfuerzo. El personal de la armada considera que la asistencia en la toma de decisiones es un aspecto relevante, puesto que los sistemas de inteligencia artificial pueden actuar como herramienta de apoyo, proporcionando análisis de datos detallados que ayudan en la toma de decisiones estratégicas, sobre todos en aquellas situaciones críticas en las que la velocidad y la precisión son realmente esenciales[52].

### 4.2.1. La inteligencia artificial en la toma de decisiones estratégicas

La toma de decisiones estratégicas en la defensa nacional se refiere al proceso sistemático a través del cual los líderes y responsables de la seguridad de un país, desarrollan, evalúan y seleccionan cursos de acción para proteger la integridad territorial, la soberanía y los intereses nacionales frente a amenazas y desafíos tanto internos como externos. Este proceso incluye las siguientes acciones: identificación de amenazas, formulación de estrategias, asignación de recursos, coordinación intergeneracional y con aliados internacionales, evaluación continua, etc.[53].

En este sentido, la relación entre la inteligencia artificial y la toma de decisiones estratégicas es cada vez más estrecha, puesto que la inteligencia artificial puede ofrecer herramientas avanzadas que mejoren significativamente la efectividad y la eficiencia de los procesos de defensa[54]. Los lideres nacional están incorporando herramientas de inteligencia artificial en sus estrategias de seguridad nacional y programas militares, de diferentes formas.

En primer lugar, a través de sistemas de aprendizaje supervisado, que se utiliza para tareas como la clasificación o predicción, por ejemplo, para identificar amenazas potenciales basadas en datos históricos.

En segundo lugar, sistemas de aprendizaje no supervisado, que deviene muy útil para el análisis de patrones y la detección de anomalías, como la identificación de actividades inusuales en el ciberespacio. Además, estos enfoques de aprendizaje profundo pueden identificar eficientemente varios tipos de anomalías en sistemas informáticos modernizando los sistemas de detección de intrusiones y permitiendo a los algoritmos reconocer patrones y comportamientos novedosos. Tal y como reportan diversos estudios, este sistema ha sido especialmente exitoso en la identificación y prevención de actividades maliciosas como el fraude y las intrusiones[55].

---

52. Conde de los Ríos, A., «La armada ante la revolución de la inteligencia artificial», en *Cuadernos de pensamiento naval*, año 24, núm. 37 (primer cuatrimestre), 2024, pág. 134.

53. Machado, J.L., «Strategic Decisions-Making in National Defense», en *Revista Científica de la Escuela Superior de Guerra del Ejército*, vol. III, núm. 2, noviembre 2024, pág. 59.

54. Ídem.

55. Últ. ob. cit., pág. 64.

En tercer lugar, destacan los sistemas derivados de aprendizaje por refuerzo. Estos se utilizan en simulaciones y escenarios de entrenamiento donde los algoritmos aprenden a tomar decisiones óptimas a través de prueba y error. Unido a ello, el aprendizaje por refuerzo está centrado en la resolución de problema secuenciales de toma de decisiones mediante ensayo y error. Los algoritmos pueden aplicarse a estados continuos utilizando técnicas de aproximación. De otro lado, algunos desafíos incluyen la escalabilidad a espacios de alta dimensión y la necesidad de grandes cantidades de datos para aprender políticas útiles[56].

Por último, los sistemas basados en agentes de inteligencia artificial, que se utilizan para mejorar la toma de decisiones, entre otras acciones. A través de estos sistemas es posible analizar grandes cantidades de datos, simular escenarios complejos y proporcionar a los comandantes recomendaciones en tiempo real. Estas herramientas permiten a los agentes simular combates escenarios de guerra, permitiendo a los comandantes practicar y refinar sus estrategias sin riesgos reales. Además, los soldados y oficiales pueden entrenarse en entornos virtuales controlados por sistemas de inteligencia artificial, mejorando sus habilidades tácticas y la toma de decisiones[57].

Un ejemplo de este tipo de sistemas sería *Aegis,* que influye significativamente en los ciclos de decisión y acción. Este tipo de sistemas han demostrado la capacidad de la inteligencia artificial para comprimir de decisión, asignando recursos de manera eficiente en situaciones de alta complejidad[58].

### 4.2.2. La inteligencia artificial en el contexto armamentístico y de misiones militares

El aprendizaje profundo puede revertir gran utilidad a la hora de analizar grandes conjuntos de datos y detectar la presencia de armamento en imágenes o vídeos. Esto será de gran utilidad en escenarios de defensa, donde la detección temprana de amenazas es crucial[59]. De otro lado, la inteligencia artificial puede desempeñar un papel muy importante en la fase de preparación y planificación de misiones militares. De esta manera, a través de la modelización de comportamientos especiados tanto de unidades amigas, como enemigas, la inteligencia artificial permite a los comandantes evaluar su capacidad para llevar a cabo misiones, identificar posibles debilidades y anticipar situaciones futuras[60]. En el ámbito de apoyo al mando, la inteligencia artificial puede operar de dos maneras principales: (i) supervisando en

56. Últ. ob. cit., págs. 64, 65.

57. Últ. ob. cit. pág. 65.

58. Conde de los Ríos, A., ob. cit., pág. 142.

59. Últ. ob. cit., pág. 142.

60. Últ. ob. cit., pág. 142.

segundo plano tareas como la conducción automática de enjambres de drones o la fusión de datos de inteligencia; (ii) presentando un papel fundamental en la fusión de datos de múltiples dominios, como pueden ser: aire, espacio, tierra, mar o ciberespacio. Autores destacan que este enfoque es esencial para una representación precisa de la realidad y la eficacia operativa[61].

Otro ámbito es el que este tipo de sistemas se traducen en grandes ventajas en áreas como la navegación y el control de sistemas, donde la complejidad y fragmentación de datos pueden convertirse en un obstáculo a la hora de la toma de decisiones. Un ejemplo de ello NAIAD de Navantia, que es un sistema para el control de los sistemas no tripulados de la Armada. Más allá, la Marina de Estados Unidos (US Navy) está explorando activamente el uso de la inteligencia artificial para mejorar diversos aspectos de las operaciones navales, como la guerra de información, la cadena de muerte táctica y las prácticas sanitarias para los operadores navales[62]. Por último, los sistemas de detección de amenazas basados en inteligencia artificial han demostrado su capacidad para analizar grandes cantidades de datos de sensores con la finalidad de identificar posibles amenazas. En este sentido, la OTAN está desarrollando su propia inteligencia artificial para consulta de documentos llamada *AI Content Learning Alerts and Insights Review,* también conocido como *AI Claire.* A través de este sistema, se emite una notificación a los usuarios sobre nueva información de su interés[63].

## 5. Desafíos emergentes de la inteligencia artificial

Dentro de los principales riesgos, encontramos despersonalización de las decisiones judiciales, difícil acceso al código fuente y falta de interoperabilidad. Empezando por el sector judicial, algunos autores han criticado que, las decisiones judiciales emitidas gracias a estos sistemas de inteligencia artificial, sustituyendo en cierta manera a los jueces, harían realmente difícil la identificación de un sujeto a la hora de atribuirle su posible responsabilidad civil derivada de los daños y perjuicios generados por error o mal funcionamiento de la herramienta[64]. Sin embargo, caben diversas soluciones ante este desafío[65].

61. Últ. ob. cit., pág. 144.

62. Últ. ob. cit., págs. 145-146.

63. Últ, ob. cit., pág. 147.

64. Pineros Polo, E. ob. cit., pág. 71.

65. Aunque exista cierta preocupación a la hora de exonerar a una posible víctima por potenciales daños derivados del uso de estos sistemas, con la nueva Directiva en materia de productos defectuosos 2024/2853, que considera al software como producto, las víctimas podrán obtener su indemnización a través de esta vía, pese a que la prueba del defecto continue teniendo cierto carácter «diabólico», pese a las facilidades probatorias

En segundo lugar, destaca la doctrina que el uso del algoritmo en el contexto de un juicio penal no debe obstaculizar el ejercicio del derecho de defensa. De esta manera, señalan que el principio de igualdad de armas y la presunción de inocencia pueden verse amenazados por la inteligencia artificial en los procesos penales. En este sentido, destacan que es fundamental garantizar que el interesado tenga acceso a los datos utilizados por la inteligencia artificial para poder impugnar cualquier conclusión errónea de la herramienta predictiva. También destacan que, en cuanto al derecho de acceso del algoritmo, existe una diferente latente entre Europa y Estados Unidos. Mientras que las autoridades judiciales estadounidenses siguen siendo reacias a reconocer plenamente este derecho y a equilibrar los intereses privados, en Europa el marco es más protector debido al RGPD, mencionado anteriormente, que establece un derecho a la información sobre la lógica que subyace en los procesos penales, respetando al mismo tiempo el principio de igualdad de armas y la presunción de inocencia[66].

De otro lado, respecto al uso de la inteligencia artificial en el contexto militar, la doctrina considera que plantea desafíos significativos. En este sentido, destacan la necesidad de mantener el control humano sobre las decisiones críticas, la gestión de la «niebla de guerra» y la adaptación de las dinámicas cambiantes del campo de batalla. Además, la inteligencia artificial debe ser diseñada para ser interoperable y adaptarse a las diferentes culturas militares, pudiendo garantizar su eficacia en coaliciones internacionales[67].

## 6. Responsabilidad civil derivada de un posible daño

Una vez analizados cuáles son los diversos usos de la inteligencia artificial en cuanto a la toma de decisiones estratégica se refiere, y habiendo advertido de alguno de sus posibles riesgos, en el último epígrafe de este trabajo nos encargaremos de apuntar brevemente, a través de ligeras pinceladas, quién, cómo y a través de que vía se deberá responder en caso de que estos sistemas terminen ocasionando un resultado que no era el inicialmente deseado. Pensemos en una herramienta de ataque completamente autónoma, que ha sido configurada de manera errónea y causa resultados indebidos. O en el caso de la justicia robotizada en el sector administrativo, qué ocurre si a través de la información errónea proporcionada por un sistema de este tipo, se causan unos daños irreparables.

introducidas en este nuevo instrumento. En este sentido, véase Aparicio Araque, B., «Responsabilidad civil por daños causados por sistemas de neurotecnología e inteligencia artificial», en *Revista CESCO de Derecho de Consumo*, núm. 54/2025, 2025.

66. Ninón Sánchez Ronceros, I., «La implementación de la inteligencia artificial en las decisiones judiciales en procesos penales», en *CHORNANCAP Revista Jurídica del Ilustre Colegio de Abogados de Lambayeque*, vol. 1, núm. 2, julio-diciembre 2023, págs. 45-46.

67. Conde de los Ríos, A., ob. cit., pág. 144.

Respecto a la primera cuestión, con la entrada en vigor de la nueva Directiva en materia de productos defectuosos[68] se ha resuelto, en parte, este gran debate mantenido durante años. Al considerar al software como producto, la parte perjudicada tendrá legitimación activa más que suficiente para demandar al fabricante de dicho producto. Sin embargo, en este caso nos encontraremos con una serie de problemas tanto en la fase probatoria, como a la hora de evitar la aplicación de las cláusulas de exoneración.

Respecto a la prueba, en este caso puede hablarse de la conocida como *probatio* diabólica. Si bien es cierto que en los artículos 9 y 10 se han introducido unos mecanismos de facilidad de la actividad probatoria, recogiendo una seria de presunciones del nexo causal y de la defectuosidad del producto, nos seguimos encontrando con tipos de sistemas poco transparentes, conocidos como de «caja negra», en los que la aportación de cualquier prueba es un hecho realmente obstaculizador a la hora de obtener una demanda. En este sentido, se propuso en instrumentos legislativos anteriores, que este tipo de responsabilidad fuese objetiva, pero la presión de las empresas tecnológicas y el posible desincentivo de la inversión en innovación hicieron que este tipo de responsabilidad quedase descartado.

En relación con las cláusulas de exoneración, se recogen en el artículo 11, y la que resulta más problemática teniendo en cuenta este tema en concreto, es la conocida como «cláusula de exoneración por riesgos del desarrollo», recogida en el apartado 6. En este sentido, no deberá responder el fabricante si puede probar *«que el estado objetivo de los conocimientos científicos y técnicos en el momento en que el producto fue introducido en el mercado, puesto en servicio o durante el período en el que el producto estaba bajo el control del fabricante no permitía detectar el carácter defectuoso».* Esto, al hablar de sistemas completamente autónomos que se retroalimentan y que, pasados unos meses de aprendizaje, pueden llegar a desarrollar funciones inesperadas, en un gran impedimento a la hora de resarcir un daño causados por estos sistemas.

En cuanto a la segunda cuestión, habría que estudiar si esa información defectuosa que proporciona el sistema sería suficiente para considerar al producto como defectuoso. Como ejemplo, sería la situación siguiente: se cuenta con un sistema de IA generativa avanzado, al que se le pide ayuda en un contexto militar. La herramienta proporciona una determinada información, incluyendo consejos. El equipo sigue estos consejos, pero el resultado no es el esperado y fallecen todos, incluidos el equipo atacante. El primer caso que se planteó en nuestro país de la información incorrecta como fundamento de responsabilidad fue el del buque *Urquiola,* resuelto por la STS (3ª), de 18 de

68. Directiva (UE) 2024/2853 del Parlamento Europeo y del Consejo, de 23 de octubre de 2024, sobre responsabilidad por los daños causados por productos defectuosos y por la que se deroga la Directiva 85/374/CEE del Consejo. DOUE núm. 2853, de 18 de noviembre de 2024.

julio de 1983 (RJ 1983/4065)[69]. En el presente caso, la defectuosa información de la carta de navegación fue el fundamento de la responsabilidad de la Administración pública. Esta cuestión se planteó también en la STJUE, de 10 de junio de 2021[70], conocida como caso Krone, y la cuestión a dilucidar en el presente caso es si constituye un producto defectuoso un periódico impreso que, tratando de un tema paramédico, da un consejo de salud inexacto[71].

Del fallo obtenido en estas resoluciones, podemos sacar las siguientes conclusiones. Si la información errónea forma parte de uno de los elementos clave (también denominados intrínsecos) del producto que constituye su soporte, podremos considerar que el producto es defectuoso. De esta manera, el criterio que regirá en esta cuestión es el de la valoración de la esencialidad del servicio de la información[72].

## 7. Conclusiones

Tal y como se ha analizado a lo largo del presente trabajo, la inteligencia artificial se ha convertido en un instrumento indispensable en diversos ámbitos del sector público, como son la toma de decisiones judiciales y la defensa de la seguridad nacional. Pese a haber analizado las múltiples ventajas que reportan estos sistemas en la toma de decisiones y en la gestión militar, no hemos de obviar los desafíos que acechan actualmente y que deben ser mitigados, como son: la falta de transparencia de estos sistemas, la presencia de sesgos en las decisiones automatizadas, el derecho a reconocer el código fuente del algoritmo que motiva la toma de decisiones judiciales, así como la presencia de un ser humano que supervise este tipo de sistemas cuando se produce la toma de esas decisiones. Si bien es cierto que actualmente se han promulgado varios instrumentos normativos, algunos ya en vigor, como es el

69. En la que el TS consideró que el capitán había cumplido correctamente sus deberes, y que su fallecimiento fue causado por «una sucesión temporal de acontecimientos», que empezó con «el primer choque de la quilla de dicho barco ocasionada por el anormal funcionamiento del servicio público de cartografía marina y de información sobre el mar y litoral».

70. VI c. KRONE-Verlag Gesellshaf mbH & Co KG, C-65/20. En la misma se planteaba la responsabilidad de la empresa editora de un periódico en el cual se publicaba una sección con consejos de salud, escrita por un miembro de una orden religiosa experto en hierbas medicinales. En la columna de 31 de diciembre de 2016 se recomendaba a las personas con dolor remático que, después de frotar la zona afectada con aceite graso o manteca de cerdo, se colocaran una capa de rábano picante durante dos y cinco «horas», pero hubo un error y deberían haber escrito «minutos». A las tres horas, la demandante tuvo que retirarse el ungüento debido a que sentía un fuerte dolor causado por una reacción cutánea tóxica.

71. STJUE apartado 24.

72. García-Micó, T. G., *Robótica Quirúrgica y derecho de daños*, ed. Marcial Pons, Madrid, 2024, págs. 73-74.

Reglamento de IA, y otros que entrará en vigor en 2026, como en la Directiva 2024/2853, actualmente nos encontramos en una situación de incertidumbre normativa debido a la gran cantidad de instrumentos que se proponen en materia de inteligencia artificial, no viendo todos la luz. Como solución, puede plantearse una vía alternativa, como es el desarrollo de normativa de carácter sectorial, que permita aportar respuestas prácticas en diferentes sectores, lo que reportará en definitiva una mayor seguridad jurídica. Todo ello en aras a desmitificar la inteligencia artificial como una enemiga imparable, pues realmente se puede convertir en una gran aliada, siempre y cuando se hago un uso diligente y adecuado de la misma.

# BIBLIOGRAFÍA

**Alkorta Idiakez, I.,** «La discriminación algorítmica en el sector sanitario», en *Inteligencia artificial y derecho de daños: cuestiones actuales. Acorde al Reglamento (UE) 2024/1689*, obra colectiva, coordinadores Moreno Martínez, Juan A. y Femenía López, Pedro J., ed. Dykinson, Madrid, 2024.

**Aparicio Araque, B.,** «Responsabilidad civil por daños causados por sistemas de neurotecnología e inteligencia artificial», en *Revista CESCO de Derecho de Consumo*, núm. 54/2025, 2025.

**Aragäo Seia, C**., «Inteligencia artificial: responsabilidad civil 3.0», en *El impacto de la era digital en el derecho*, obra colectiva, coordinador Quiroga Corti, M.P., director López Ulla J. M., ed. Aranzadi, Pamplona, 2023.

**Ayllon García, J. D.,** «La inteligencia artificial como medio de difusión y control de la fake news», en *El derecho en la encrucijada tecnológica, Estudios sobre derechos fundamentales, nuevas tecnologías e inteligencia artificial*, ed. Tirant Lo Blanch, Valencia, 2022.

**Barona Vilar, S**., *Algoritmización del derecho y de la justicia: de la Inteligencia Artificial a la Smart Justice*, Ed. Tirant Lo Blanch, Valencia, 2021.

**Berlanga de Jesus, A**., «El camino desde la inteligencia artificial al Big Data», en *Revista de Estadística y Sociedad*, núm. 68, 2016.

«Cláusula y Reglas de Disputas de Inteligencia Artificial (23 abril 2024)», en *Diario LA LEY*, 3 de octubre de 2024.

**Conde de los Ríos, A**., «La armada ante la revolución de la inteligencia artificial», en *Cuadernos de pensamiento naval*, año 24, núm. 37 (primer cuatrimestre), 2024.

**Cornago Baratech J.F**., «El papel de la inteligencia artificial en la defensa nacional», en *Inteligencia artificial y defensa. Nuevos horizontes*, ed. Aranzadi, Navarra, 2021.

**Cotino Hueso, L.**, *Derechos y garantías ante la inteligencia artificial y las decisiones automatizadas*, ed. Aranzadi, Navarra, 2022.

**De Lara- García, J.,** «Inteligencia Artificial y Judicial: Experiencias en América Latina», en *DIVULGARE, Boletín Científico de la Escuela Superior de Actopan*, Publicación semestral, vol. 9, núm. 17, 2022.

**Espinosa, P., Clemente, M.,** «La percepción de la toma de decisiones a través de inteligencia artificial cuando se produce daño a las personas», en *Estudios Penales y Criminológicos,* Universidad de Santiago de Compostela, núm. 44, 2023.

**Jiménez Cardona, M**., «Aplicación de la inteligencia artificial en la toma de decisiones jurisdiccionales (España)», en *Revista Quaestio Iuris*, Rio de Janeiro, vol. 16, núm. 03, 2023

**López Rincón, D**., «Robots y abogacía», en *Derecho de los Robots*, director Moisés Barrio Andrés, Ed.Wolters Kluwer, Madrid, 2018.

**Machado, J. L.**, «Strategic Decisions-Making in National Defense», en *Revista Científica de la Escuela Superior de Guerra del Ejército*, vol. III, núm. 2, noviembre 2024, pág. 59.

**Martín Rodriguez, G.,** «Nuevos horizontes en las políticas de la UE en materia de inteligencia artificial: hacia el Derecho Europeo de la IA», en *La atribución de una responsabilidad jurídico penal e internacional de la inteligencia artificial*, obra colectiva, directora Beatriz García Sánchez, coordinador Jiménez García, Francisco, ed. Iustel, Madrid, 2023.

**Navas Navarro, S.** y otros, *Inteligencia artificial: tecnología y derecho,* Ed. Tirant lo Blanch, Valencia, 2017.

**Ninón Sánchez Ronceros, I**., «La implementación de la inteligencia artificial en las decisiones judiciales en procesos penales», en *CHORNANCAP Revista Jurídica del Ilustre Colegio de Abogados de Lambayeque*, vol. 1, núm. 2, julio-diciembre 2023.

**Pineros Polo, E.,** «El juez-robot y su encaje en la constitución española. La inteligencia artificial utilizada en el ámbito de la toma de decisiones por los tribunales», en *Estudios de Deusto*, Universidad de Deusto, vol. 72/1, enero-junio 2024.

**Pino Diez, R**., *Introducción a la inteligencia artificial: sistemas expertos, redes neuronales artificiales y computación evolutiva*, Universidad de Oviedo, servicio de publicaciones, 2002.

**Portellano, P**., «Inteligencia Artificial y responsabilidad por productos*»,* en *Revista de Derecho Mercantil,* núm. 316/2020, Editorial Civitatis, S.A., 2020.

**Reyes López, M.J**., «La protección al consumidor al hilo de las nuevas propuestas legislativas comunitarias», en *Actualidad Civil*, núm. 7, editorial LA LEY, julio de 2023.

**Salazar García, I.,** «Retos actuales de la ética en la inteligencia artificial», en *Derechos y garantías ante la inteligencia artificial y las decisiones automatizadas*, obra colectiva, director Lorenzo Cotino Hueso, ed. Aranzadi, Navarra, 2022.

# MATRIZ IC-IP: UNA HERRAMIENTA PARA APOYAR LA PROSPECTIVA ELECTORAL EN EMPRESAS INTERNACIONALIZADAS

**Pablo Las Heras**

*Analista (Responsable) de Inteligencia en INECO*

## 1. Introducción

Que los procesos electorales tienen un impacto alto en la situación de un país, desde el sector económico hasta el ámbito de la seguridad, es algo asumido en el ámbito de la empresa española internacionalizada. Pero el potencial impacto específico de unas elecciones en un país extranjero en las operaciones a corto, medio y largo plazo de una empresa internacionalizada no siempre se tiene en cuenta a la hora de proceder a la toma de decisiones.

Los escenarios postelectorales pueden tener un impacto mucho más profundo, continuado y rupturista que la simple afectación al normal funcionamiento de una sociedad que provoca, durante unos días o semanas, un proceso electoral al uso. Unas elecciones pueden suponer cambios de interlocutores públicos, inversiones o recortes presupuestarios, aceleración, ralentización o incluso cancelación de proyectos en curso. Y estos cambios que, más allá de que puedan no ser inmediatos, están directamente relacionados con esa jornada electoral.

Muchos de los sectores —sector bancario, grandes infraestructuras, telecomunicaciones, energía, etc.— en los que empresas españolas están internacionalizadas están ampliamente participados, cuando no directamente intervenidos, por el Estado. Esta cuestión supone que el escenario que se abre al día siguiente del escrutinio sea clave para las operaciones de una empresa en ese determinado país.

Además, en este tipo de sectores se da una paradoja: a menudo los ciclos de vida de proyectos e inversiones en el extranjero son mucho más largos que los ciclos políticos del país donde se realiza dicho proyecto o inversión, generándose un cierto nivel de incertidumbre que, aunque se puede paliar a nivel contractual, rara vez se hace irrelevante. Un caso arquetípico que ilustra esta paradoja son los grandes proyectos de infraestructura, cuyo ciclo de desarrollo (desde sus primeros planteamientos hasta la finalización de su ejecu-

ción) a menudo abarca más de una década, cuando un ciclo electoral típico no abarca más de 4 o 5 años.

Teniendo en cuenta estas cuestiones, aquellos familiarizados con el ámbito de la inteligencia llegarán a una conclusión obvia: la prospectiva, aplicada a los procesos electorales de aquellos países donde una empresa lleva a cabo su labor, es una herramienta de altísimo valor para la toma de decisiones empresariales de carácter estratégico en una empresa internacionalizada. Como señalan Godet y Duarnce: «En un mundo en mutación donde las fuerzas de cambio están revolucionando los factores de inercia y los hábitos instalados, se impone un esfuerzo creciente de prospectiva (tecnológica, económica y social) a la empresa para dotarse de flexibilidad estratégica, es decir para reaccionar con flexibilidad manteniendo su rumbo»[1].

Aunque la solución —la prospectiva— a la incertidumbre que supone el impacto de los procesos electorales en la operativa de una empresa parece sencilla, su aplicación al ámbito empresarial no resulta tan fácil de implementar. La prospectiva, como técnica central de la inteligencia, debe estar incluida en el ámbito de la empresa; pero la prospectiva, como técnica, tiene un desarrollo académico que la hace poco encajable en los tiempos y costumbres que los decisores tienen en el ámbito empresarial. La amplísima literatura existente en torno a la prospectiva, aunque vital para mantener una práctica estructurada de esta herramienta, tampoco solventa esta dicotomía con facilidad, hace falta adaptar la teoría a la práctica.

El presente trabajo tiene por objetivo intentar resolver esa dicotomía, presentando una metodología prospectiva vinculada específicamente al ámbito electoral que aspira a cumplir con un doble objetivo:

a) Mantener una estructura teórica coherente con las múltiples obras que desarrollan la prospectiva en general y las técnicas de análisis de inteligencia en particular, para hacerla replicable por la comunidad de inteligencia que trabaja en el ámbito de la empresa.

b) Adaptarse a las necesidades que tiene el ámbito ejecutivo de las empresas —que es el ámbito con la responsabilidad de la toma de decisiones estratégicas—, de cara a facilitar su consumo.

Una metodología basada en:

a) La priorización de eventos electorales a analizar, con el fin de evitar el gasto de recursos —siempre escasos— en situaciones de bajo impacto potencial.

b) En la generación de escenarios para aquellas situaciones que sí se consideren rentables en términos de consumo de recursos/impacto potencial.

1. Godet, M., Durance, P., *Prospectiva estratégica: problemas y métodos*, 2.ª ed., Donostia-San Sebastián, Prospektiker, Cuaderno n.º 20, 2007, pág. 13.

# 2. Marco teórico y conceptual

La metodología que aquí se propone se apoya en tres tradiciones bien asentadas: la prospectiva, la inteligencia aplicada y el análisis político-electoral. De estas metodologías es de las que toma conceptos y técnicas que, adaptadas al ámbito corporativo, permiten anticipar el impacto de procesos electorales sobre empresas internacionalizadas.

En la presente sección no se pretende una revisión exhaustiva de la extensa teoría existente al respecto, sino un encuadre breve y funcional que proporcione el sustrato conceptual necesario para comprender y valorar la metodología expuesta en los apartados siguientes.

## 2.1. Prospectiva y anticipación estratégica

La prospectiva se entiende aquí como la exploración sistemática de futuros plausibles con el propósito de mejorar las decisiones presentes bajo incertidumbre, distinguiéndola explícitamente de cualquier pretensión de «acertar» el futuro. Su contribución específica consiste en abrir el abanico de posibilidades (explorar escenarios), hacer explícitas las hipótesis que sostienen cada futuro posible y ordenar la conversación estratégica en torno a implicaciones y puntos de decisión[2].

En la práctica, la literatura ha consolidado una caja de herramientas (métodos de escenarios, *Delphi, backcasting, horizon scanning*, entre otros) que pueden combinarse según el problema y las restricciones de tiempo y recursos[3]. En el ámbito corporativo, el valor de la prospectiva no reside tanto (generalmente por falta de tiempo, recursos y, porque no admitirlo, cultura de la inteligencia) en producir grandes informes de largo plazo, sino en articular procesos de anticipación reutilizables, capaces de informar decisiones ejecutivas en ciclos cortos sin perder rigor metodológico; esta idea de adaptación al consumo ejecutivo ha sido subrayada previamente en el contexto español[4].

## 2.2. Inteligencia aplicada y técnicas estructuradas

La inteligencia aplicada se concibe como un proceso orientado a la decisión (dirección, obtención, análisis, difusión) cuyo fin es reducir la incerti-

2. Godet, M., *Strategic Foresight: La Prospective, problémes et méthodes*, n.º 10, París, UNESCO, 2009, págs. 42-43.

3. Glenn, J. C., Gordon, T. J., *Futures Research Methodology, Version 3.0*, Washington D.C., Millennium Project, 2009.

4. Las Heras, P., «La prospectiva para consumo ejecutivo. Necesidad de adaptar la disciplina al producto», comunicación presentada en el Congreso *Análisis de Inteligencia y Prospectiva*, Grupo de Estudios en Seguridad Internacional, Universidad de Granada, 8-9 de abril de 2019. Disponible en: https://www.ugr.es/~gesi/congreso/comunicacion29-5.pdf

dumbre del decisor. En entornos complejos, las técnicas estructuradas ayudan a disciplinar el juicio experto y mitigar sesgos: entre ellas, el Análisis de Hipótesis Competitivas (ACH), los modelos de valoración multicriterio (*scoring* cualitativo/ponderado), las matrices comparativas o los ejercicios de red *teaming*[5]. Estas técnicas no sustituyen la experiencia del analista, pero obligan a explicitar criterios, evidencias e inferencias, mejorando la trazabilidad del razonamiento y la reproducibilidad de los resultados[6].

En el terreno específico de la prospectiva electoral corporativa, la utilización de una valoración estructurada por criterios —por ejemplo, escalas ordinales para evaluar relevancia del contexto y exposición de la empresa— es coherente con los enfoques de análisis multicriterio empleados tanto en inteligencia como en gestión de riesgos[7]. Esta lógica hace más objetiva y entendible, por parte del decisor, la priorización y prepara la construcción de escenarios, que en nuestra propuesta es el núcleo del proceso: una vez valorados contexto y posición, el equipo de inteligencia genera escenarios propios de impacto y orienta el nivel de seguimiento y profundidad analítica que corresponde a cada caso.

## 2.3. Análisis político, sistemas electorales y efecto empresa

Los arreglos institucionales y los sistemas electorales configuran los incentivos de los actores y condicionan los resultados de gobierno (mayorías, coaliciones, bloqueos), por lo que no basta con «quién gana»: importa cómo se gobierna[8]. En democracias consolidadas, variables como fragmentación, polarización, reglas de investidura o la distribución territorial del poder alteran de manera sensible la probabilidad de parálisis o de giros regulatorios[9].

Para empresas internacionalizadas en sectores altamente intervenidos (infraestructuras, energía, transporte), estos cambios se traducen en licen-

5. Heuer, R. J., Pherson, R. H., *Técnicas analíticas estructuradas para el análisis de inteligencia*, Madrid, Plataforma de Inteligencia y Seguridad (i+k), 2015, págs. 81-86, 175-184 y 253-255.

6. Heuer, R. J., *Psychology of Intelligence Analysis*, Washington D.C., Center for the Study of Intelligence, 1999, pp. 28-52 Clark, R. M.: *Intelligence Analysis: A Target-Centric Approach*, Washington D.C., CQ Press, 2007.

7. Heuer, R. J., Pherson, R. H.: *Técnicas analíticas estructuradas para el análisis de inteligencia*, Madrid, Plataforma i+k, 2015; Keeney, R. L. y Raiffa, H.: *Decisions with Multiple Objectives: Preferences and Value Tradeoffs*, Cambridge, Cambridge University Press, 1993.

8. Sartori, G., *Ingeniería constitucional comparada. Una investigación de estructuras, incentivos y resultados*, Madrid, Alianza Editorial, 1994, págs. 19-58; Lijphart, A.: *Patterns of Democracy: Government Forms and Performance in Thirty-Six Countries*, New Haven, Yale University Press, 1999, pp. 130-170.

9. Dahl, R. A., *Poliarquía. Participación y oposición*, Madrid, Tecnos, 1989, pp. 13-41.

cias, presupuestos, cronogramas de obra, regulación sectorial, contratación pública y, en general, en el riesgo político-operativo que afecta a la ejecución y al flujo de caja de proyectos de ciclo largo. De ahí la necesidad de un método específico que conecte el análisis institucional-electoral con la exposición concreta de la empresa y que permita anticipar escenarios de impacto operativamente relevantes[10].

Este marco explica por qué la metodología que se presenta integra, de manera explícita, la evaluación del contexto político-electoral y la evaluación de la posición corporativa, como dos pilares que, combinados, permiten priorizar esfuerzos y activar la generación de escenarios cuando corresponde.

# 3. Metodología propuesta

Asumiendo el reto de que dotar a una empresa de una prospectiva útil no es fácil, a lo largo de mi carrera como analista de inteligencia he llegado a desarrollar un método que, puesto en práctica, funciona como una herramienta funcional y altamente valorada en la toma de decisiones. Una herramienta cuyo objetivo no es predecir resultados, sino dar al decisor certidumbre respecto a los escenarios que se abren ante un proceso de estas características —que son cíclicos y sobre los que apenas se puede intervenir— y que además tiene la flexibilidad suficiente para no convertirse en un protocolo automático y sortear la limitación de recursos, tan común en los departamentos de inteligencia de la empresa privada.

Esta metodología de análisis se basa, en primer lugar, en el análisis combinado de dos variables, el Índice de Contexto (IC) y el Índice de Posición (IP), ambos con un *scoring* de 0 a 4, con el objetivo de establecer la importancia que un determinado proceso electoral tiene para la empresa. Una vez integrados ambos análisis en una matriz (matriz contexto-posición), se establece un rango a partir del cual se procede a un procedimiento clásico de generación de escenarios cuyo resultado será el entregable para el decisor.

## 3.1. Fase 1: Análisis de contexto

La primera fase de esta metodología es el análisis de contexto, que tiene por objetivo establecer un *scoring* a través de una serie de preguntas guía respecto al posible impacto de unas elecciones en base al contexto de las propias elecciones. Una vez puntuadas, en una escala de 0 a 4, las preguntas guía establecidas, se realiza una media aritmética para establecer el Índice de Contexto (IC), que se establecerá entre 0 a 4.

10. Nohlen, D., *Sistemas electorales y partidos políticos*, México D.F., Fondo de Cultura Económica, 1998, pp. 70-120.

Debido a la flexibilidad de la que hace gala esta metodología, las preguntas guía son abiertas y maleables en función del tipo de empresa, tanto en su número — aunque se recomienda no ser inferior a tres ni superior a seis — como en su planteamiento — pudiéndose adaptar en función de las circunstancias o criterios del analista/decisor.

Dicho esto, es importante mantener el criterio de que las preguntas guía estén, específicamente, vinculadas al contexto electoral y no a otras cuestiones. Para ejemplificar esta fase, se proponen las siguientes preguntas guía:

a) ¿Las elecciones se dan en instituciones con competencias en el sector de la empresa? Donde se puntuaría con un 0 en caso de que no (por ejemplo, unas elecciones presidenciales en un país donde la gran mayoría de las competencias se encuentran en el poder legislativo, como en Polonia), hasta un 4 en caso de que si (unas elecciones regionales donde las competencias en la materia —pongamos proyectos de infraestructuras— están fuertemente descentralizadas, como en EE. UU.).

b) ¿Son unas elecciones competidas? Donde un 0 correspondería a unos comicios donde el resultado se da prácticamente por hecho con antelación (Reino Unido 2024) y un 4 a unas elecciones con opciones de gobernabilidad muy abiertas (Países Bajos 2023).

c) ¿Hay un escenario de gobernabilidad claro? Donde un 0 correspondería a un si evidente (caso de unas elecciones presidenciales donde sólo puede haber un ganador) a un 4 en caso negativo (elecciones parlamentarias altamente fragmentadas y sin alianzas postelectorales claras).

## 3.2. Fase 2: Análisis de posición

Siguiendo la misma metodología que en el análisis de contexto (preguntas guía, contestadas en una escala ascendente de 0 a 4), la segunda fase trata de establecer cuál es la posición corporativa de la empresa en el marco de los comicios (Índice de Contexto). Posición corporativa amplia, entendiendo como tal tanto el nivel micro (proyectos u oportunidades específicos), como a nivel supraempresarial (empresa nacional —española en el caso que nos ocupa—, empresa extranjera en un país X); pasando por supuesto por la posición de la propia empresa en cuestión.

De nuevo, esta fase tiene que contar con un amplio nivel de maleabilidad para que el analista y/o decisor tengan capacidad de adaptar la metodología a la práctica; pero es importante mantener el criterio de que las preguntas guías de esta sección estén centradas específicamente en la empresa (por mucho que esa posición sea amplia) en el contexto electoral.

En este sentido, y a modo de ejemplo, se plantean a continuación las siguientes preguntas guía:

a) ¿Concurren a las elecciones actores beligerantes contra la empresa/país/proyecto de interés? Puntuándose con 0 una respuesta claramente negativa y con 4 una claramente positiva.

b) El/los proyecto/s de interés. ¿Son centrales (en negativo o positivo) en el marco de la conversación electoral? Puntuándose con 0 cuando el/los proyecto/s tengan una importancia nula en los comicios y un 4 cuando sean centrales en el marco de las discusiones electorales (por ejemplo, cuando un proyecto de infraestructura y su realización o cancelación son promesa electoral de uno de los contendientes, como pasó en México 2016 con el Nuevo Aeropuerto Internacional de México (NAIM)).

c) ¿Existen narrativas indirectas que podrían afectar significativamente los intereses de la empresa en el país en el que se celebran los comicios? Puntuándose con 0 en caso negativo y con 4 en caso de que existan y sean relevantes (típicamente, discursos relativos a austeridad, recortes presupuestarios, cuestiones ecológicas, protección de empresas nacionales, etc.).

## 3.3. Fase 3: Integración. Matriz contexto-posición

Una vez realizado el análisis de contexto (fase 1) y posición (fase 2) se tienen los elementos suficientes para establecer la relevancia de las elecciones para la empresa y decidir, así, el nivel de recursos que se sigue usando (o se ahorra) en su análisis. Para apoyar esta decisión se integran ambos análisis en una matriz, en la que el eje X corresponde al Índice de Contexto (IC) y el eje Y al Índice de Posición (IP). Al estar ambos índices ubicados entre 0 y 4, se generan cuatro cuadrantes (Q) de igual tamaño y posición:

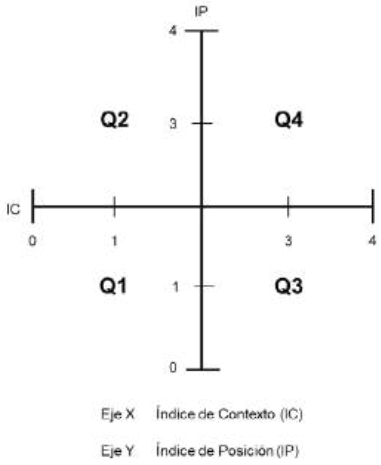



Figura 1. Matriz contexto/posición

Estos cuatro cuadrantes son los que permiten al analista valorar el nivel de relevancia (y esfuerzo posterior que requieren) unos determinados comicios; considerándose que unas elecciones que se ubiquen en el cuadrante 1 (Q1) como de bajo interés (pues requiere que tanto el IC como el IP sean inferior a 2) y unas que se ubiquen en el cuadrante 4 (Q4), que requiere un IC y un IP superior en ambos casos a 2, como de alto interés; con dos cuadrantes intermedios (Q2 y Q3).

A continuación se presenta un ejemplo de aplicación para ilustrar el uso de esta herramienta metodológica en estas primeras fases. Tenemos elecciones en el país Z y H, produciéndose los siguientes resultados en las preguntas guías de IC e IP:

| **Elecciones Z** | | **Elecciones H** | |
|---|---|---|---|
| Índice de Contexto (IC): **1,6** | | Índice de Contexto (IC): **3,3** | |
| P1 | 1 | P1 | 4 |
| P2 | 3 | P2 | 3 |
| P3 | 1 | P3 | 3 |
| Índice de Posición (IP): **2,6** | | Índice de Posición (IP): **3,6** | |
| P1 | 2 | P1 | 4 |
| P2 | 3 | P2 | 4 |
| P3 | 3 | P3 | 3 |

Posicionándose en la matriz contexto/posición de la siguiente manera:

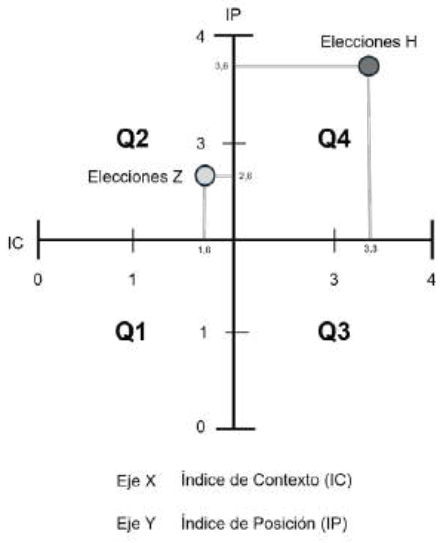



Figura 2. Ejemplo de ubicación de dos elecciones en la matriz contexto—posición (IC-IP), a partir de los valores obtenidos en las preguntas guía de IC e IP.

El uso de esta matriz permite por tanto establecer de una forma altamente intuitiva, pero metodológicamente robusta, el nivel de relevancia para la empresa que tienen unos determinados comicios, tanto a nivel individual como comparativamente. En el caso propuesto como ejemplo, resulta evidente que las elecciones de H se vislumbran como claramente más relevantes que las de Z, que sólo tendrían un índice de riesgo importante (>2) en el Índice de Posición (IP).

### 3.4. Fase 4: Culminación. Generación de escenarios

Una vez ubicada la importancia del proceso electoral en cuestión esta metodología termina con la aplicación de una de las técnicas más usadas —y estudiadas— en el ámbito de la inteligencia: la generación de escenarios. No es objeto de este trabajo establecer que método para generar escenarios debe usarse. Cualquiera de las múltiples herramientas disponibles para este propósito (como la construcción de escenarios narrativos, el análisis STEEPV o la técnica *Delphi*, aunque esta última sea difícilmente aplicable al contexto corporativo) son válidas, y el uso de una u otra depende del criterio del analista, la disponibilidad de recursos y el acuerdo con el decisor en cual y en qué entregable los escenarios electorales apoyan de manera más eficaz la toma de decisiones. Si es pertinente mencionar, no obstante, que el uso previo de la matriz IC-IP dota a esta última fase de la prospectiva electoral de una serie de facilitadores relevantes:

a) La priorización de recursos hacia elecciones que se consideren realmente relevantes (que no tienen por qué ser únicamente las encuadradas en el Q4, pudiendo decidirse, por ejemplo, que una determinada actividad económica tiene una alta sensibilidad a cualquier cambio político y considerar relevantes también aquellas elecciones ubicadas en el Q3).

b) El análisis previo de factores relevantes en metodologías de generación de escenarios como el STEEPV (especialmente los factores políticos que operan en un determinado país).

c) Coordinación con el decisor respecto a la pertinencia del proceso de generación de escenarios, pudiendo actuar la matriz IC-IP como una alerta temprana que permita al analista generar interés en el decisor respecto al producto final de la generación de escenarios.

## 4. Ventajas y límites

Ahondando en la cuestión de la pertinencia y utilidad de esta herramienta —recordemos, la matriz IC-IP, no en genérico la generación de escenarios— creo adecuado empezar a cerrar esta explicación hablando de las fortalezas, o ventajas, así como de sus límites; basado principalmente en la experiencia adquirida poniendo en práctica esta herramienta.

## 4.1. Ventajas y fortalezas

El uso de la matriz IC-IP no se limita a entender un proceso electoral como un evento donde lo importante es el resultado —es decir, quien gana— sino que permite enfocarlo centrado en el impacto real y específico que unos comicios pueden tener sobre proyectos y la empresa, desde el impacto operativo que decisiones como la cancelación de un proyecto puede tener, a el impacto reputacional potencial que hay en el hecho de que una empresa/proyecto sea un tema central en las discusiones preelectorales, aunque finalmente no se produzca un impacto operativo.

Además, al ser un proceso parametrizado —flexible, pero parametrizado al fin y al cabo— se convierte en trazable, replicable y fácilmente entendible por parte del decisor, incentivando su implicación y participación en las fases iniciales de análisis y permitiendo al analista justificar decisiones internas (como la priorización de recursos) frente a la empresa. Esto es altamente positivo para fortalecer la que muchas veces es la parte más frágil del ciclo de la inteligencia[11] —porque su éxito no depende sólo del analista/equipo de inteligencia— que es la difusión y el posterior feedback; proporcionando una clara ventaja competitiva frente a procesos más ad-hoc o intuitivos que, aunque pueden ser plenamente funcionales, son más complicados de explicar y/o difundir.

En síntesis, a nivel de ventajas, el uso de la matriz IC/IP permite al analista ordenar el análisis prospectivo electoral y justificar tanto sus decisiones respecto a la priorización de recursos como la pertinencia de los análisis más amplios que se produzcan como consecuencia de ese primer análisis.

## 4.2. Límites y advertencias

Como todo sistema, el uso de la matriz IC-IP no está exento de límites, si bien cabe mencionar que estos no son exclusivos de esta metodología. El primer límite que mencionar es un viejo conocido de todo analista de inteligencia: la dependencia de la calidad de los inputs[12] utilizados para encarar fases 1 (análisis de contexto) y 2 (análisis de posición) de esta metodología. Es cierto que esta cuestión está mitigada debido a la naturaleza de los propios procesos electorales, que son públicos y rara vez adolecen de falta de información (más bien todo lo contrario). Pero también lo es que son procesos que pueden adolecer de pocas certezas —incluso de cambios de guion no predecibles—

11. Lowenthal, M. M., *Intelligence: From Secrets to Policy*, Washington D.C., CQ Press, 2015, cap. 3 (*The Intelligence Process — The Intelligence Cycle*); Clark, R. M.: *Intelligence Analysis: A Target-Centric Approach*, Washington D.C., CQ Press, 2007, caps. 1-2.

12. Heuer, R. J., *Psychology of Intelligence Analysis*, Washington D.C., Center for the Study of Intelligence, 1999, caps. 1-2.

en cuestiones clave, como son el nivel de cumplimiento de programas electorales o la configuración final de las alianzas postelectorales; cuestiones que pueden restar solidez al *scoring* inicial.

Otro clásico «mal» que afecta a todo analista de inteligencia es de los sesgos cognitivos de él mismo[13]. Aunque la estructuración de la matriz IC-IP permite mitigar estos sesgos, el juicio del analista —y por lo tanto sus sesgos— sigue siendo la fuerza fundamental que articula el proceso de *scoring*, lo que la expone a ser atravesada por dichos sesgos, pudiendo comprometer su solidez.

Por último, cabe destacar que esta herramienta no está pensada para sustituir o enfocar las decisiones estratégicas del decisor —como a menudo, y mi juicio erróneamente, se pretende exigir a la inteligencia corporativa—, al menos en la fase de la matriz IC-IP. La matriz aporta un elemento estructurado de análisis respecto a *qué puede pasar*, pero no entra a analizar el *qué se debe hacer*. Sin perjuicio de que esta cuestión se pueda abordar en la fase 4 de generación de escenarios, la realidad es que tal y como está planteada, la matriz IC/IP no funciona como una llamada a la acción en relación a la propia empresa (aunque si lo haga en relación al proceso interno de la inteligencia corporativa).

Los límites por tanto, a pesar de existir:

a) No son ajenos a los que habitualmente cualquier unidad de inteligencia encuadrada en una empresa se encuentra.

b) Son perfectamente manejables y mitigables con base a la amplia literatura existente al respecto.

## 4.3. Recomendaciones de uso

Una de las claves para implantar con éxito esta herramienta es la de mantener la flexibilidad, que constituye uno de los rasgos más valiosos de la matriz IC-IP. Igual que no todas las elecciones requieren el mismo esfuerzo ni nivel de detalle —cuestión que la matriz IC/IP ayuda a discernir— no todas las situaciones requieren las mismas preguntas, ni todas las matrices tienen por qué exigir las mismas respuestas. En este sentido, aplicar de manera rígida el método puede terminar generando un uso ineficiente de la herramienta.

Una segunda cuestión clave es la estandarización. La matriz funciona mejor cuando se aplican plantillas homogéneas y criterios consistentes a lo largo del tiempo y entre distintos analistas. Ello no solo mejora la calidad técnica del producto, sino que facilita la comparación longitudinal entre proce-

13. Heuer, R. J., *Psychology of Intelligence Analysis*, Washington D.C., Center for the Study of Intelligence, 1999, caps. 2-4.

sos electorales diferentes y reduce la dependencia de estilos individuales. De este modo, se consigue que la herramienta no sea únicamente el reflejo del juicio de un analista concreto en un momento determinado, sino un procedimiento común de la unidad de inteligencia.

Aunque estas dos características —flexibilidad por un lado y estandarización por otro— pudieran parecer contradictorias, la clave del éxito en la implementación de la matriz IC-IP reside, justamente, en encontrar el equilibrio entre estas dos cuestiones; dando libertad al analista para amoldar la herramienta al caso, pero también dar certidumbre al decisor respecto a que el trabajo del analista se basa en algo más estructurado que su mera voluntad. Otro elemento que destacar es la importancia de la comunicación, que está vinculada a esta última cuestión. La matriz IC-IP o un conjunto de escenarios prospectivos carecen de valor si no se presentan de manera clara y comprensible para el decisor.

Traducir el análisis en productos que no sólo describan lo que puede pasar, sino que permitan identificar con facilidad implicaciones concretas y niveles de riesgo, es un requisito para que la herramienta cumpla su función de apoyo real a la toma de decisiones. Por ello, tener un catálogo de productos diverso pero concreto, que deriven del análisis inicial realizado en base a la matriz, es altamente recomendable. Como ejemplo ilustrativo de este catálogo basado en la matriz, se ofrece lo siguiente:

a) Para elecciones situadas en el cuadrante Q1: Nota (2-3 párrafos) vía correo electrónico comunicando que la elección se considera intrascendente para la compañía y exponiendo motivos principales y fin de seguimiento electoral.

b) Para elecciones situadas en los cuadrantes Q2 y Q3: Nota breve en formato PDF (1-2 páginas) analizando de forma breve el elemento de riesgo (IC o IP) y el potencial impacto general de las elecciones en la compañía. Seguimiento electoral superficial.

c) Para elecciones situadas en el cuadrante Q4: Informe de escenarios y potencial impacto completo (4-8 páginas) y seguimiento electoral profundo y prioritario.

En definitiva, la matriz IC-IP no debe entenderse como un ejercicio accesorio ni como una herramienta aislada, sino como un mecanismo que permite transformar la incertidumbre electoral en un análisis estructurado, comprensible y útil para la empresa. Su valor radica tanto en ordenar el trabajo del analista como en dotar al decisor de un producto coherente con sus necesidades, para convertir la prospectiva electoral en una pieza plenamente integrada en la inteligencia corporativa. Precisamente porque sus fortalezas se complementan con límites conocidos y con recomendaciones claras de uso, esta metodología no se agota en el plano técnico, sino que abre la puerta a consolidar la prospectiva electoral como una función estable y necesaria dentro de la práctica empresarial.

## 5. Conclusiones

La prospectiva electoral no debe confundirse con un ejercicio de predicción ni con un intento de anticipar de manera exacta el resultado de unas elecciones. Se trata, más bien, de un proceso estructurado que permite explorar posibles impactos sobre la empresa y sus proyectos, y de este modo dotar al decisor de una herramienta de anticipación que, sin eliminar la incertidumbre, la ordena y la hace manejable. La anticipación, y no la predicción, es por lo tanto el terreno natural de la prospectiva aplicada al ámbito corporativo.

La metodología propuesta se articula en torno a dos pilares —el análisis del contexto electoral y el análisis de la posición corporativa— que, una vez cuantificados de forma estructurada, permiten situar cada proceso en una matriz sencilla pero robusta.

Esa matriz no es un fin en sí mismo, sino una primera capa de análisis que facilita priorizar el esfuerzo, discriminar qué comicios exigen un seguimiento intensivo y cuáles pueden resolverse con un producto más ligero, y ofrecer al decisor un marco claro y replicable para comprender por qué se recomienda invertir más o menos recursos en un caso concreto.

La lógica de la matriz, además, es la de servir de disparador para fases más ambiciosas dentro del ciclo de inteligencia. Una de sus principales virtudes es que establece las condiciones que justifican la generación de escenarios, que debería ser consecuencia natural de este análisis inicial y no una actividad disociada. Al vincular la matriz con la prospectiva de escenarios se consigue que el trabajo del analista tenga continuidad, evitando que se quede en un diagnóstico estático y permitiendo que se convierta en un proceso dinámico y adaptativo.

A pesar de las limitaciones señaladas —dependencia de inputs de calidad, posible influencia de sesgos, necesidad de criterio experto— considero que la herramienta es altamente útil. Su fortaleza no radica en eliminar el juicio del analista, sino en dotarlo de un marco que lo ordena, lo hace trazable y lo comunica de forma eficaz. En ese sentido, no sustituye a la decisión estratégica del decisor, pero sí mejora de manera sustantiva la calidad de la información sobre la que esa decisión se apoya.

Otra virtud destacable es su carácter replicable y adaptable. La matriz IC-IP puede ser aplicada en unidades de inteligencia privada con distinto grado de madurez: desde aquellas que ya tienen consolidada la prospectiva electoral, hasta las que desean iniciarse en ella. En ambos casos, el método aporta un esquema sencillo que se puede sofisticar progresivamente, incorporando indicadores cuantitativos o técnicas más avanzadas a medida que se disponga de recursos.

Finalmente, cabe subrayar que este enfoque no debe quedar encapsulado. Su mayor potencial reside en integrarse en procesos más amplios de inteligencia corporativa, en diálogo con las funciones de seguridad, gestión de

riesgos o *compliance*. La prospectiva electoral, aplicada con esta metodología, deja de ser un añadido ocasional y se convierte en un elemento estable de la práctica empresarial, capaz de reforzar la resiliencia de las organizaciones frente a un entorno político cada vez más incierto.

## BIBLIOGRAFÍA

**Clark, R. M.**, *Intelligence Analysis: A Target-Centric Approach*, Washington D.C., CQ Press, 2007.

**Dahl, R. A.**, *Poliarquía. Participación y oposición*, Madrid, Tecnos, 1989.

**Glenn, J. C.**, **Gordon, T. J.**, *Futures Research Methodology, Version 3.0*, Washington D.C., Millennium Project, 2009.

**Godet, M.**, *Strategic Foresight: La Prospective, problémes et méthodes*, París, UNESCO, 2009.

**Godet, M.**, **Durance, P.**, *Prospectiva estratégica: problemas y métodos*, 2.ª ed., Donostia-San Sebastián, Prospektiker, Cuaderno n.º 20, 2007.

**Heuer, R. J.**, *Psychology of Intelligence Analysis*, Washington D.C., Center for the Study of Intelligence, 1999.

**Heuer, R. J.**, **Pherson, R. H.**, *Técnicas analíticas estructuradas para el análisis de inteligencia*, Madrid, Plataforma de Inteligencia y Seguridad (i+k), 2015.

**Keeney, R. L.**, **Raiffa, H.**, *Decisions with Multiple Objectives: Preferences and Value Tradeoffs*, Cambridge, Cambridge University Press, 1993.

**Lijphart, A.**, *Patterns of Democracy: Government Forms and Performance in Thirty-Six Countries*, New Haven, Yale University Press, 1999.

**Lowenthal, M. M.**, *Intelligence: From Secrets to Policy*, Washington D.C., CQ Press, 2015.

**Nohlen, D.**, *Sistemas electorales y partidos políticos*, México D.F., Fondo de Cultura Económica, 1998.

**Sartori, G.**, *Ingeniería constitucional comparada. Una investigación de estructuras, incentivos y resultados*, Madrid, Alianza Editorial, 1994.

# EPÍLOGO

Epilogar es siempre causa de satisfacción. Significa que una nueva criatura sale a la luz. En este caso la alegría es doble, cuando los padres de la misma han formado parte de la familia de alumnos a lo que has tenido el privilegio de acompañar en la senda del conocimiento. La obra en cuestión es un excelente marco de estudio y reflexión sobre dos cuestiones fundamentales para comprender y sobrevivir en el mundo actual: la inteligencia y la toma de decisiones.

Según los expertos tomamos más de 35.000 decisiones al día, en función de nuestro entorno social y laboral. Muchas de ellas inconscientes, pero otras, asumiendo que la opción elegida puede acarrear graves consecuencias. Elegir es renunciar. Para comprender esta aseveración en este mundo tan complejo, y prepararnos para un más complejo futuro, es necesario analizar cómo han evolucionado los medios y formas de obtención, cómo se interrelacionan con la necesidad de generar inteligencia y cómo todos ellos, pueden influir en un adecuado proceso de toma de decisiones. Los capítulos de esta obra nos guiarán por esta senda.

La inteligencia, como proceso mental, ha sido uno de los principales motores del desarrollo de los seres vivos. La capacidad para adquirir, procesar y utilizar información ha permitido a los organismos adaptarse, sobrevivir y prosperar en entornos cambiantes. Los primeros humanos dependían de la información para su existencia. En ausencia de comunicación verbal y escrita, los indicios y el lenguaje no verbal, eran la base para obtener esa información. La inteligencia cognitiva (COGNINT) era, por tanto, la base de esa obtención.

El desarrollo del sistema nervioso central permitió a los organismos no solo reaccionar, sino también anticiparse a los eventos. La inteligencia, entonces, dejó de ser solo una respuesta inmediata y se convirtió en una herramienta de planificación, estrategia y base de la decisión. Con el desarrollo del lenguaje verbal, y posteriormente de la escritura, aumentaron las dimensiones de producción y las formas de obtención de información; así como la conciencia de vulnerabilidad, si esos datos pudieran ser empleados por entes hostiles. La comunicación era, y es, fundamental y desarrollarla hoy en el área de la inteligencia es un reto.

Con el surgimiento de las civilizaciones, la inteligencia humana se convirtió en un fenómeno colectivo. La inteligencia ya no era solo una característica

individual, sino un sistema compartido. La obtención de información en fuentes abiertas se potenció y la accesibilidad a parte de esa información se fue conformando en OSINT, ya empleada en los primeros tiempos, y potenciada con los nuevos. La contrastación de la veracidad era cada vez más importante, tanto como lo es hoy la figura de analista 4.0. Por otro lado, parte de la información debía mantenerse en secreto y con ello proteger los datos propios y desvelar los ajenos, surgieron la CLOSINT y la contrainteligencia.

Las relaciones humanas se hicieron más complejas y las fuentes humanas fueron cogiendo más fuerza (HUMINT), el desarrollo de identidades culturales, bien sociales, bien políticas, bien religiosas generó la potenciación de la obtención de inteligencia por medio de parámetros culturales (CULTINT) para, entre otras, prevenir y evitar la radicalización. No basta con obtener información, hay que hacerlo no solo bajo normas y leyes, también cumpliendo con la ética. El dinero, o su similar según la época, se consolidó como un pilar del desarrollo, y con ello se hizo fundamental el avance de la inteligencia económica, del control del gasto, y del seguimiento del blanqueo de capitales.

Se hizo necesario el poder obtener/proteger todos esos complejos sistemas y la inteligencia de señales, SIGINT, se fue abriendo camino como una forma fundamental de generar inteligencia. El desarrollo de tecnologías satelitales condujo a la inteligencia geoespacial o GEOINT. La tecnología trajo consigo el materialismo y se dejó a un lado la biosfera, eclosionó, como necesaria, una rama de la inteligencia con conciencia de protección del medio ambiente.

A través de la observación, la experimentación y la lógica, se desarrollaron teorías que explicaban el mundo. En la actualidad, esta capacidad ha alcanzado nuevas dimensiones con la aparición de la inteligencia artificial, expandiendo los límites de lo que entendemos por conocimiento e información. Esta evolución, tanto biológica como tecnológica, ha transformado profundamente la forma en que accedemos y utilizamos la información. Por lo que el reto se agudiza ante la ingente cantidad de información y la necesidad de verificar la autenticidad de esta, la IA ha multiplicado exponencialmente este proceso y se ha ido conformando en una nueva dimensión, la AMINT.

Vivimos en una era donde el acceso a la información parece ilimitado, gracias a la digitalización y la inteligencia artificial. La toma de decisiones se hace cada vez más difícil, gracias a, y pese a, la gran cantidad de fuentes a las que tenemos acceso y al inundante flujo de información que nos rodea. Pero esto no basta, es necesario adelantarse al futuro mediante herramientas de prospectiva.

Tras este corto recordatorio evolutivo, destacar que la obra que tiene en sus manos realiza un excelente recorrido que abarca: desde la importancia de la inteligencia de nuestro vecino ibérico, la evolución de la normativa de inteligencia, la ética, la nueva figura del analista 4.0, la inteligencia econó-

mica, las finanzas, el blanqueo de capitales, la sostenibilidad, los procesos de radicalización, la jurisprudencia, la comunicación en inteligencia, la piratería, la prospectiva electoral, hasta el impredecible futuro de la IA.

Esta obra dirigida por Diego González López y editada por COLEX, presenta una herramienta de visión holística que ayudará al lector a comprender las diferentes dimensiones de la realidad global en la comunidad de los analistas de inteligencia, así como en los niveles de decisión. Todas ellas son cuidadosamente tratadas en este valioso análisis interdisciplinar. Felicitar a los autores, al director y a todos aquellos que con su profesionalidad e ilusión han hecho posible que podamos aprender y deleitarnos con un documento tan valioso.

Madrid, septiembre de 2025.

**Manuel González Hernández**

*Teniente Coronel de artillería*
*Doctor por la Universidad de Granada*
*Profesor de la Escuela de Guerra del Ejército*

# INTELIGENCIA Y TOMA DE DECISIONES: PERSPECTIVAS ACTUALES

*Inteligencia y toma de decisiones: perspectivas actuales* es una obra colectiva que explora cómo la inteligencia, entendida como una disciplina en la toma de decisiones en el sector público y privado, se adapta a los desafíos del mundo contemporáneo. A través de la mirada de distintos especialistas, el libro recorre perspectivas clave como la ética, el impacto de la inteligencia artificial, la seguridad energética, la seguridad medioambiental, la radicalización en prisiones o la prospectiva electoral. También analiza la evolución normativa en materia de información clasificada, los desafíos existentes en el ámbito de la Unión Europea, la relevancia de la comunicación estratégica y el perfil del nuevo analista de inteligencia. El resultado es una visión amplia, rigurosa y actual que combina conocimientos y reflexión académica con aplicaciones y experiencias prácticas. Un recorrido imprescindible para entender cómo se toman decisiones en un escenario global complejo, donde la inteligencia no es opcional, sino el recurso estratégico necesario para afrontar la volatilidad.

---


## DIRECCIÓN

Diego González López

## AUTORÍA

Joaquín González López, Andrea Andreu Gutiérrez, Alejandro López Palma, César Augusto Giner Alegría, Patrick Salvador Peris, Carlos Álvaro Peris, Albero Camarero Orive, Alejandra Moreno García, Susana Berrocal Díaz, Diego González López, Irene Gil Matos, Inmaculada Crespo González, Patricia Pérez Rodríguez, Raquel Pinilla Gómez, Fernando Ibáñez Gómez, João Miguel Oliveira Narciso, Yago González Quinzán, Raquel Alamà Perales, Blanca Aparicio Araque, Pablo Las Heras.



ISBN: 979-13-7011-370-4

9 791370 113704

O.A.