Capítulo primero

Aplicación de la inteligencia económica en la lucha contra la delincuencia organizada y la delincuencia grave

Antonio Balas Dávila

Sumario

El concepto de seguridad, en los últimos veinte años, se ha venido expandiendo, alcanzando la generalidad de los ámbitos y de los espacios, tanto reales como virtuales. Esta circunstancia se enmarca en el difuso y omnipresente fenómeno de la globalización, la «hiperconectividad» y el desarrollo exponencial de las tecnologías.

En este contexto, la inteligencia se erige en fundamental para cualquier estrategia de seguridad. Sin embargo, la complejidad y especificidad inherente a cada ámbito de interés, requiere de una inteligencia especializada. En este sentido, la seguridad económica es un elemento esencial de la seguridad nacional y, por tanto, requiere una inteligencia *ad hoc*.

Es precisamente en el marco de la seguridad nacional donde la inteligencia económica coadyuva en la lucha contra la delincuencia organizada y grave, detectando de manera temprana, patrones inusuales en un determinado sector productivo, transacciones sospechosas o la aparición de elementos anómalos en un concreto contexto mercantil.

Palabras clave

Seguridad económica, Inteligencia económica, Delincuencia organizada y grave, Globalización, Seguridad nacional.

Application of economic intelligence in the fight against organized crime and serious crime

Abstract

Over the past two decades, the notion of security has broadened considerably, extending across virtually all domains and spaces, both physical and virtual. This expansion is intricately linked to the pervasive dynamics of globalization, hyper-connectivity, and the exponential advance of technology.

In this environment, intelligence becomes indispensable to any security strategy. Yet the complexity and specificity of each domain call for specialized approaches. Within this framework, economic security stands as a core dimension of national security and thus demands tailored intelligence.

Economic intelligence, in turn, plays a pivotal role in the National Security system by supporting the fight against serious and organized crime. It does so through the early identification of atypical patterns in productive sectors, suspicious transactions, and the emergence of anomalous elements in commercial contexts.

Key words

Economic security, Economic intelligence, Serious and organized crime, Globalization, National security.

Lista de abreviaturas

AEAT	Agencia Estatal de Administración Tributaria
AI	Artificial Intelligence / Inteligencia Artificial
AML	Anti-Money Laundering / Lucha contra el blanqueo de capitales
AMLA	Autoridad Europea contra el Blanqueo de Capitales
AML/CFT	Anti-Money Laundering / Countering the Financing of Terrorism (lucha contra el blanqueo de capitales y contra la financiación del terrorismo)
ASEAN	Asociación de Naciones del Sudeste Asiático / The Association of Southeast Asian Nations
AVE	Asociación Valenciana de Empresarios
BC	Blanqueo de Capitales
BCE	Banco Central Europeo
BdE	Banco de España
BfV	Bundesamt für Verfassungsschutz / Oficina Federal para la Protección de la Constitución (Alemania)
BI	Business Intelligence / Inteligencia de negocios
BM	Banco Mundial
BRICS	Brasil, Rusia, India, China y Sudáfrica
CAEID	Curso de Altos Estudios de Inteligencia y Defensa
CCAA	Comunidades Autónomas
CCN-CERT	Centro Criptológico Nacional – Computer Emergency Response Team
CE	Constitución Española
CEOE	Confederación Española de Organizaciones Empresariales
CEPYME	Confederación Española de la Pequeña y Mediana Empresa
CI	Competitive Intelligence / Inteligencia Competitiva
CIDOB	Barcelona Centre for International Affairs (en catalán Centre d'Informació i Documentació Internacionals a Barcelona).
CIFAS	Centro de Inteligencia de las Fuerzas Armadas

CITCO	Centro de Inteligencia contra el Terrorismo y el Crimen Organizado
CMN	Corporaciones Multinacionales
CNMC	Comisión Nacional de los Mercados y la Competencia
CNMV	Comisión Nacional del Mercado de Valores
CNI	Centro Nacional de Inteligencia
CNP	Cuerpo Nacional de Policía
CNPIC	Centro Nacional de Protección de Infraestructuras Críticas
COREPER	Comité de Representantes Permanentes (del Consejo de la UE)
CPFF	Consejo de Política Fiscal y Financiera
CPI	Corte Penal Internacional
CSN	Consejo de Seguridad Nacional
DGEIPYME	Dirección General de Estrategia Industrial y de la Pequeña y Mediana Empresa
DG TAXUD	Dirección General de Fiscalidad y Unión Aduanera (Comisión Europea)
DG TRADE	Dirección General de Comercio (Comisión Europea)
DG	Delincuencia Grave
DO	Delincuencia Organizada
DSN	Departamento de Seguridad Nacional
EARTO	Asociación Europea de Organizaciones de Investigación y Tecnología / European Association of Research and Technology Organisations
EBA	European Banking Authority / Autoridad Bancaria Europea
EE.UU.	Estados Unidos (de América)
EES	Estrategia Española de Seguridad (2011)
EFECC	European Financial and Economic Crime Centre (Centro de Europol contra la delincuencia financiera y económica)
EFIPPP	Europol Financial Intelligence Public Private Partnership / Asociación Público-Privada de Inteligencia Financiera de Europol

EIOPA	European Insurance and Occupational Pensions Authority / Autoridad Europea de Seguros y Pensiones de Jubilación
EMPACT	European Multidisciplinary Platform Against Criminal Threats (Plataforma Multidisciplinar Europea contra las Amenazas Criminales)
ENCODG	Estrategia Nacional contra el Crimen Organizado y la Delincuencia Grave
EPPO	European Public Prosecutor's Office / Fiscalía Europea
ESCB	European System of Central Banks / Sistema Europeo de Bancos Centrales
ESMA	European Securities and Markets Authority / Autoridad Europea de Valores y Mercados
ESN	Estrategia de Seguridad Nacional
ESRB	European Systemic Risk Board / Junta Europea de Riesgo Sistémico
EU INTCEN	EU Intelligence and Situation Centre (Centro de Inteligencia y Situación de la UE)
EUIPO	European Union Intellectual Property Office (Oficina de Propiedad Intelectual de la UE)
EUROJUST	Agencia de la Unión Europea para la Cooperación Judicial Penal
EUROPOL	European Union Agency for Law Enforcement Cooperation / Agencia de la Unión Europea para la Cooperación Policial
EUMS INT	Intelligence Directorate of the EU Military Staff (Dirección de Inteligencia del Estado Mayor de la UE)
EU SOCTA	EU Serious and Organised Crime Threat Assessment (Evaluación de Amenazas de Crimen Grave y Organizado de la UE)
FDI	Foreign Direct Investment (Inversión extranjera directa – IED)
FEDEA	Fundación de Estudios de Economía Aplicada
FEDER	Fondo Europeo de Desarrollo Regional

FEDIT	Federación Española de Centros Tecnológicos
FEMP	Federación Española de Municipios y Provincias
FGE	Fiscalía General del Estado
FIU	Financial Intelligence Unit / Unidad de Inteligencia Financiera
FMI	Fondo Monetario Internacional
FSE	Fondo Social Europeo
FSR	Financial Stability Review (Informe de Estabilidad Financiera del BCE)
G8	Grupo de los Ocho
G20	Grupo de los Veinte
G77	Grupo de los Setenta y Siete (ONU)
GAFI / FATF	Grupo de Acción Financiera Internacional / Financial Action Task Force
GATT	General Agreement on Tariffs and Trade / Acuerdo general sobre Aranceles Aduaneros y Comercio
GRECO	Grupo de Estados contra la Corrupción (Consejo de Europa)
HFC	Hybrid Fusion Cell (Célula de Fusión Híbrida de la UE)
HUMINT	Human Intelligence / Inteligencia de Fuentes Humanas
I+D+i	Investigación + Desarrollo + innovación
IASN	Informe Anual de Seguridad Nacional
IBEX	Índice Bursátil Español
IE	Inteligencia Económica
IED/FDI	Inversión Extranjera Directa
IF	Inteligencia Financiera
INCIBE	Instituto Nacional de Ciberseguridad
INE	Instituto Nacional de Estadística
INTERPOL	International Criminal Police Organization / Organización Internacional de Policía Criminal

IPCR-ISAA	Integrated Political Crisis Response / Integrated Situational Awareness and Analysis
IVA	Impuesto sobre el Valor Añadido
LEAs	Law Enforcement Agencies (Fuerzas y Cuerpos de Seguridad)
LECrim	Ley de Enjuiciamiento Criminal
LOSU	Ley Orgánica del Sistema Universitario, aprobada en España en 2023 (Ley Orgánica 2/2023, de 22 de marzo)
LRBRL	Ley Reguladora de las Bases del Régimen Local
MAIC	Máster en Análisis de Inteligencia y Ciberinteligencia
MERCOSUR	Mercado Común del Sur
MITI	Ministry of International Trade and Industry / Ministerio de Industria y Comercio exterior
MRR	Mecanismo de Recuperación y Resiliencia (instrumento central de la UE para canalizar los fondos Next Generation EU)
MTIC	Missing Trader Intra-Community / Fraude intracomunitario de comercio
MUR	Mecanismo Único de Resolución
MUS	Mecanismo Único de Supervisión
OCDE	Organización para la Cooperación y el Desarrollo Económico
OCC	Oficina de Coordinación de Ciberseguridad
OCDE	Organización para la Cooperación y el Desarrollo Económicos
OCTA	Organised Crime Threat Assessment (antiguo documento de Europol) / Evaluación de la amenza del Crimen Organizado
OEPM	Oficina Española de Patentes y Marcas
OIIE	Observatoire International de l'Intelligence Économique / Observatorio Internacional de Inteligencia Económica
OLAF	Oficina Europea de Lucha contra el Fraude

OMC	Organización Mundial del Comercio
ONG	Organización No Gubernamental
ONI	Oficina Nacional de Investigación de Aduanas e Impuestos Especiales (AEAT)
ONIF	Oficina Nacional de Investigación del Fraude (AEAT)
ONU	Organización de las Naciones Unidas
ORGA	Oficina de Recuperación y Gestión de Activos
OSCE	Organización para la Seguridad y la Cooperación en Europa
OSINT	Open Source Intelligence / Inteligencia de Fuentes Abiertas
OTAN	Organización del Tratado del Atlántico Norte
OUA	Organización para la Unidad Africana
PBC/FT	Prácticas de Blanqueo de Capitales y Financiación del Terrorismo
PENTRA	Plan Estratégico Nacional contra la Trata y la Explotación de Seres Humanos
PESC	Política Exterior y de Seguridad Común (de la UE)
PIB	Producto Interior Bruto
PIF	Informe sobre la Protección de los Intereses Financieros de la UE
PNUMA	Programa de las Naciones Unidas para el Medio Ambiente
PRTR	Plan de Recuperación, Transformación y Resiliencia
pymes	Pequeñas y medianas empresas
REF	Régimen Económico y Fiscal (de Canarias)
RECI	Red Española de Ciudades Inteligentes
RIS3	Research and Innovation Strategies for Smart Specialisation / Estrategias Regionales de Especialización Inteligente
ROI	Registro de Operadores Intracomunitarios
RSC	Responsabilidad Social Corporativa

RTO	Research and Technology Organisations / Organizaciones de Investigación y Tecnología
SATCEN	European Union Satellite Centre / Centro de Satélites de la UE
SEAE / EEAS	Servicio Europeo de Acción Exterior / European External Action Service
SEPBLAC	Servicio Ejecutivo de la Comisión de Prevención del Blanqueo de Capitales e Infracciones Monetarias
SEPI	Sociedad Estatal de Participaciones Industriales
SESF	Sistema Europeo de Supervisión Financiera
SGAE	Sociedad General de Autores y Editores
SIAC	Capacidad Única de Análisis e Inteligencia / Single Intelligence Analysis Capacity
SIE	Sistema de Inteligencia Económica
SIGINT	Signals Intelligence / Inteligencia de Señales
SOCTA	Serious and Organised Crime Threat Assessment (véase EU SOCTA) / Evaluación de la amenaza de la Delincuenica Grave y Organizada
STS	Sentencia del Tribunal Supremo
SVA	Servicio de Vigilancia Aduanera (AEAT)
TFM	Trabajo Fin de Máster
TFUE	Tratado de Funcionamiento de la Unión Europea
UA	Unión Africana
UCO	Unidad Central Operativa (Guardia Civil)
UDEF	Unidad de Delincuencia Económica y Fiscal (CNP)
UE	Unión Europea
UIE	Unidad de Inteligencia Económica
UIF	Unidad de Inteligencia Financiera
UK	United Kingdom / Reino Unido
UNCTAD	United Nations Conference on Trade and Development / Conferencia de las Naciones Unidas sobre Comercio y Desarrollo

UNICRI	United Nations Interregional Crime and Justice Research Institute Institute / Instituto Interregional de las Naciones Unidas para Investigaciones sobre la Delincuencia y Justicia
UNODC	United Nations Office on Drugs and Crime / Oficina de las Naciones Unidas contra la Droga y el Delito
USA	United States of America / Estados Unidos de América
USMCA/T-MEC	United States-Mexico-Canada Agreement / Tratado entre México, Estados Unidos y Canadá
VAB	Valor Añadido Bruto
VAT	Value Added Tax / Impuesto sobre el Valor Añadido
VTTL	VAT Total Tax Liability / Responsabilidad Fiscal Total de IVA
WoS	Web of Science

1 Antecedentes

Durante los últimos veinte años, el mundo ha sufrido una serie de calamidades de afectación mundial. En este sentido, cabe destacar la crisis financiera global de 2008 (Stiglitz, 2010), la pandemia de COVID-19 (Baldwin y Weder, 2020) o los efectos del cambio climático (Nordhaus, 2013). En todos estos amargos sucesos, la componente económica ha estado siempre presente, proyectándose en las diferentes fatalidades hacia los confines más alejados, a través de una suerte de onda expansiva de esa misma naturaleza.

Este extremo se explica, en gran medida, por el proceso de la globalización contemporánea y su constituyente económico a través de diferentes hitos acaecidos, ubicados en distintos momentos del siglo xx y xxi:

- Desmantelamiento del sistema de Bretton Woods y liberalización financiera, generando una expansión de las conexiones económicas globales (Osterhammel y Petersson, 2005).
- Revolución tecnológica y digital, posibilitando una economía global interconectada, donde las interacciones sociales y económicas ya no están limitadas por la geografía o una secuencia temporal acostumbrada, emergiendo una economía basada en la información, en la capacidad de las redes para procesarla y distribuirla mundialmente, en tiempo real (Castells, 2006).
- Consolidación del neoliberalismo, facilitando la desregularización y la apertura de nuevos mercados, derivando en una reconfiguración de estructuras económicas y sociales a nivel mundial (Harvey, 2007).
- Caída del muro de Berlín, como catalizador de la expansión del capitalismo, el libre mercado y la interconexión tecnológica, llegando, incluso, a ser considerada como el punto de inicio del actual fenómeno de globalización (Friedman, 1999).
- Surgimiento de China como potencia económica, operando cambios profundos en todos los órdenes, constituyéndose en un elemento polarizante al resistirse a una occidentalización (Jacques, 2012).

Todo ello moldea un orden mundial explicado a través de las teorías constructivistas, vinculadas a las relaciones internacionales, poniendo en valor las ideas, las identidades, las normas y los

procesos sociales frente a factores materiales más propios del realismo e incluso del idealismo, asociados a teorías geopolíticas. Esta concepción puede resumirse en la famosa frase «Anarchy is what states make of it» (Wendt, 1992).

En este sentido, una vez rota la bipolaridad entre Estados Unidos (EE. UU.) y la Unión Soviética, escenificada con la caída del Muro de Berlín, aparecieron nuevas amenazas y riesgos que intensificaron la relación entre la seguridad y la defensa. La globalización y la creciente interconectividad favorecieron espacios de cooperación internacional para resolver las diferentes crisis y conflictos (Valero, 2005).

Esto fue conformando una nueva disposición mundial que supuso un fortalecimiento, expansión y redefinición de organizaciones como Organización de las Naciones Unidas (ONU), la Organización del Tratado del Atlántico Norte (OTAN) o la Unión Europea (UE), así como la institucionalización del comercio global a través de la creación de la Organización Mundial del Comercio (OMC).

De este modo, la ONU ganó protagonismo en el ámbito de la seguridad y la gobernanza global, con un sensible aumento de las misiones de paz y las intervenciones humanitarias.

La OTAN se transformó en una organización de seguridad colectiva más flexible, incorporando antiguos países del bloque soviético y realizando operaciones fuera de su área tradicional.

Del mismo modo, la UE se institucionalizó a través del Tratado de Maastricht (1992), consolidando la unión económica y monetaria con el establecimiento del euro (1999) y propiciando una Política Exterior y de Seguridad Común (PESC), ampliando, igualmente, los países miembros, a partir de 2004, sumándose países que habían permanecido bajo la influencia soviética.

Asimismo, la OMC, fundada en 1995 como sucesora del *General Agreement on Tariffs and Trade* (GATT), se configuró como la base del sistema multilateral de comercio[1]. Otras instituciones, como el Fondo Monetario Internacional (FMI) o el Banco Mundial (BM), asumieron un papel activo en la reconversión económica de Europa del Este y Rusia, promoviendo reformas de mercado.

[1] Web oficial del Ministerio de Economía, Comercio y Empresa. Política comercial de la UE. Organización Mundial de Comercio. Disponible en: https://comercio.gob.es/PoliticaComercialUE/OMCOrganismosInternacionales/Paginas/omc.aspx [Consulta: 17 abril 2025].

De igual manera, cabe reseñar la creación de la Unión Africana (UA), en 2002, con una intención más ambiciosa, desde una perspectiva continental, que la anterior Organización para la Unidad Africana (OUA), el nacimiento de la Corte Penal Internacional (CPI), en 2002, o el reforzamiento, con el Acta de París, de la Organización para la Seguridad y la Cooperación en Europa (OSCE), manteniendo un rol clave en la transición poscomunista en el control de conflictos.

En Asia, también proliferaron organizaciones que procuran fortalecer, fundamentalmente en los ámbitos de seguridad y económico, a los distintos países miembros de esa región, constituyéndose, en ocasiones, en una respuesta o alternativa a la opción proveniente de occidente (Strand *et al*., 2016).

Es decir, los distintos países se integraron en organizaciones intergubernamentales y supranacionales, cediendo, en mayor o menor medida, parte de su soberanía con el fin de alcanzar superiores cotas de desarrollo y de seguridad, admitiendo que, otorgarse normas comunes y confiar en instituciones globales para la resolución de conflictos, podrían ser vías aceptables para mantener y mejorar las cotas de bienestar y desarrollo de cada país.

Todo ello, desde un dominio casi unipolar de Estados Unidos, que generó un sistema duradero y pacífico al reducir la rivalidad hegemónica e incentivar la cooperación (Wohlforth, 1999). Estas circunstancias contribuyeron al establecimiento de un sistema mundial denominado multilateralismo[2].

Ya entrado el siglo XXI, la propia Estrategia Española de Seguridad de 2011 afirmaba que

> «España aboga por una interdependencia responsable en la que se fomenten sinergias para buscar soluciones conjuntas a los retos comunes. Ni podemos ni debemos trabajar en solitario. Como país comprometido con el desarrollo, la paz y la seguridad mundiales, España trabaja a través de la UE, la ONU, la OTAN, la OSCE, el G20 y otras organizaciones para diseñar y alcanzar un orden internacional estable que promueva la justicia, la prosperidad y la seguridad global».

[2] Entendido como una configuración institucional mediante la cual se articulan las relaciones entre tres o más Estados, sustentada en principios de conducta generalizados. Dichos principios determinan comportamientos considerados apropiados para categorías amplias de acciones, sin atender a los intereses particulares de los actores implicados ni a las exigencias estratégicas que puedan derivarse de situaciones específicas (Ruggie, 1992).

En esta dinámica de interconexión mundial, el concepto de seguridad también mutó tras la superación del bipolarismo, percibiéndose una menor amenaza en cuanto a guerras interestatales directas, emergiendo una visión holística que abarcaba distintos ámbitos como la seguridad económica, el terrorismo internacional, el crimen organizado, las migraciones, la seguridad medioambiental o la seguridad sanitaria (Buzan, 1991). Asimismo, esta interdependencia deriva en una necesidad de superar el ámbito territorial nacional, preconizado por Alberto Antón González[3] en los Cuadernos de Inteligencia, número 2, *Nuevas amenazas a la Seguridad Nacional*, como referencia última, en un sentido estricto, de la seguridad nacional.

De este modo, durante finales del siglo XX e inicios del siglo XXI se va moldeando el concepto incipiente de seguridad económica, confiriendo a factores económicos, como la competitividad industrial y la innovación tecnológica, una especial relevancia para la seguridad nacional, argumentando que una economía sólida proporciona los recursos necesarios para mantener capacidades militares y responder a amenazas externas (Neu y Wolf, 1994).

Pero adquiere un protagonismo principal después de la crisis financiera de 2008, momento en el que, mundialmente, se toma conciencia de que las fuertes interconexiones globales afectan, también, a los riegos, descubriendo vulnerabilidades (World Economic Forum, Global Risks, 2010).

Consecuentemente, las decisiones económicas influyen en la seguridad. De manera inmediata, se evidencia que el establecer una estrategia en defensa y seguridad, a largo plazo, ha de sustentarse en una acumulación planificada de recursos (Murphy y Topel, 2013).

Ampliando el foco, la inversión en innovación tecnológica, en políticas industriales y en otros sectores estratégicos determinará la consecución de esa pretendida seguridad nacional (Weiss, 2014).

De esta manera, se percibe la idoneidad de enfoques que integren consideraciones económicas en las políticas de seguridad, ya que los recursos económicos y las decisiones financieras influyen en la seguridad y la estabilidad (Silwal *et al*., 2021).

[3] Vid.https://www.defensa.gob.es/documents/2073105/2223574/articulo_3_cuaderno_inteligencia_2.pdf/0dde73a3-76e8-537d-2e29-ea2af230a0f0?t=1732100696646 [Consulta: 21 abril 2025].

En este sentido, la propia Estrategia de Española de Seguridad (EES) de 2011, establecía que la seguridad económica es un interés vital de España en cuanto elemento constitutivo del Estado. Igualmente, la Estrategia de Seguridad Nacional (ESN) de 2013 indicaba que la seguridad económica «se erige cada vez de forma más clara y patente en requisito esencial y parte integral de la seguridad nacional, debido a su repercusión en la puesta en marcha de actuaciones gubernamentales y en el bienestar de los ciudadanos».

La inteligencia y la seguridad nacional están íntimamente unidas. La inteligencia es la herramienta que permite al Estado entender el mundo y los riesgos a los que se enfrenta, mientras que la seguridad nacional es el fin último al que sirve ese entendimiento (Johnson, 2017).

Como indica la publicación de la Escuela Superior de las Fuerzas Armadas, *Cuaderno de Inteligencia 2. Nuevas amenazas a la Seguridad Nacional*, en la actualidad

> «Los riesgos y las amenazas son multidimensionales, cambiantes, difíciles de evaluar y de predecir. Esto da lugar a crisis mucho más frecuentes, más complejas, más difíciles de prever y de gestionar, que requieren actuaciones en el multidominio y donde disponer de buenos análisis de inteligencia es crítico» (Sabaté Aragonés, 2023: 13).

Este panorama muestra la significativa incidencia de la economía en los estados y en su ciudadanía, influyéndoles en múltiples aspectos. Por lo que es lógico plantearse la conveniencia de consolidar una posición donde la economía coadyuve a mantener el bienestar social y el desarrollo de los estados, protegiéndolos, a su vez, de aquellas amenazas que pudieran menoscabar esta posición.

2 La seguridad y la inteligencia económica

El panorama descrito en el apartado anterior, asociado a una suerte de multilateralismo y de cooperación internacional, en concordancia con una visión geopolítica constructivista e idealista, ha empezado a virar[4] hacia un mundo multipolar, menos colaborativo, tendente al unilateralismo.

[4] En concordancia con lo dispuesto en el Informe Anual de Seguridad Nacional (IASN) 2023 y la acción continuada de Rusia descrita en el IASN 2024.

Esta deriva menoscaba la fluidez de las relaciones comerciales internacionales y, en consecuencia, afecta negativamente a la economía desde una perspectiva global.

Esta circunstancia económica afecta a la seguridad de los países de manera determinante. En este sentido, cabe mencionar las recientes tensiones entre EE. UU. y la UE, donde el incremento de los aranceles y exigencias de índole económico, en diferentes ámbitos, realizadas por el país americano incide en la política de seguridad de la UE.

En este contexto, los países han puesto en valor la importancia de mantener una seguridad económica adecuada, que les permita cierta independencia de actuación en el ámbito nacional e internacional, favoreciendo sus intereses. Así, Estados Unidos en su Estrategia de Seguridad Nacional de 2017 afirmaba que una economía fuerte protege al pueblo estadounidense y apuntala su poder.

En España, la inteligencia está íntimamente ligada a la seguridad. Esta circunstancia se observa en la lógica y evidente relación existente entre el artículo 1 de la Ley 11/2002, de 6 de mayo, en el que se define el propósito del Centro Nacional de Inteligencia (CNI), y el artículo 3 de la Ley 36/2015, de 28 de septiembre, de Seguridad Nacional, donde se define, precisamente, la seguridad nacional.

Asimismo, de manera específica, esta ligazón se manifiesta en el artículo 9.2 de la Ley 36/2015, de 28 de septiembre, precisando que los servicios de inteligencia e información apoyarán permanentemente al Sistema de Seguridad Nacional. De tal modo, que la inteligencia se pone al servicio del mantenimiento de la seguridad nacional.

De esta manera, el Consejo de Seguridad Nacional, en su condición de Comisión Delegada del Gobierno para la Seguridad Nacional, adquiere un papel relevante como el órgano que asiste al presidente del Gobierno en la dirección de la política de Seguridad Nacional y del Sistema de Seguridad Nacional, siendo el responsable de la gestión y supervisión de este último, así como de la elaboración de las líneas estratégicas en este ámbito.

La prevalencia de esta comisión sobre otras se pone de manifiesto, también, en el propio funcionamiento de las comisiones. Pues, aunque normativamente no existe una prelación entre comisiones delegadas, es significativo que solo en la Comisión

Delegada del Gobierno para la Seguridad Nacional se prevea la asistencia del rey de España, así como el deber de ser informado anualmente. Del mismo modo, es la única comisión delegada donde por lo general se recoge que la presidencia le corresponderá al presidente del Gobierno (salvo si asiste el rey, que entonces lo preside).

2.1 Aproximación al concepto de inteligencia económica

En relación con la triple acepción realizada por Sherman Kent (1966) y Mark M. Lowenthal (2012) organización, proceso y producto, este apartado se dirigirá a delimitar el concepto de inteligencia vinculado al producto.

En este sentido, desde finales del siglo xx hasta el tiempo actual se han ido sucediendo diferentes definiciones, entre las que se podría resaltar las realizadas por Sherman Kent, en 1966, que concibe la inteligencia como el producto resultante de la recolección, procesamiento, integración, análisis, evaluación e interpretación de información disponible sobre áreas o actores de interés.

Asimismo, Jennifer E. Sims define la inteligencia como la recopilación, análisis y diseminación de información para decisores en materia de seguridad nacional (Sims y Gerber, 2005: 15), inmersos en un entorno competitivo.

Peter Gill y Mark Phythian proponen una definición funcional y relacional, que integra proceso, producto y acción para anticipar y preservar la ventaja relativa (Gill y Phythian, 2012). Mientras que Loch K. Johnson incide en el «conocimiento y preconocimiento» (Johnson, 2007: 3) como antesala de la decisión.

Rubén Arcos aporta una visión funcional orientada a la decisión y la seguridad entendiendo que la inteligencia constituye la primera línea de la defensa y la seguridad del Estado (Arcos, 2012), aportando el conocimiento especializado para que los dirigentes puedan tomar las decisiones en las mejores condiciones.

Antonio M. Díaz Fernández muestra, también, la finalidad estratégica de la anticipación y la influencia, al conferirle a la inteligencia la comprensión del entorno para anticiparse a él (Díaz Fernández, 2013) y modificarlo, en cierta medida.

En base a todo ello, y sin extenderse mucho más, se podría definir el concepto de inteligencia, en el marco de esta monografía, como un producto analítico orientado a un decisor y sobre un asunto

concreto, desarrollado mediante un ciclo (dirección/obtención/análisis/difusión) que busca reducir la incertidumbre de manera oportuna, para preservar la seguridad o la ventaja relativa del actor, así como eludir riesgos y aprovechar oportunidades.

A partir de todo lo anterior, se puede determinar que la inteligencia es un proceso que, bajo una dirección, debe ser alimentado y analizado de manera adecuada para resultar el producto inteligencia.

De este modo y en este contexto, cabe diferenciar datos, información e inteligencia, cada uno de los cuales asociado a un nivel de elaboración distinto. Los datos son unidades básicas de observación, hechos brutos o registros aislados sobre realidades específicas huérfanos de contexto. Estos datos, recopilados de distinta forma y manera conforman la materia prima inicial.

Cuando esos datos se organizan, procesan, estructuran, analizan y se interrelacionan dotándoles de un significado contextualizado, se convierten en información una vez los datos han sido interpretados. La información agrega valor al dato, pero aún no implica un juicio analítico profundo.

Finalmente, la inteligencia es el producto final resultante de someter datos e información a un riguroso proceso analítico, evaluándolos, integrándolos y proyectándolos hacia escenarios futuros, orientando todo el proceso a facilitar una decisión minorando la incertidumbre, erigiéndose por tanto la inteligencia en un conocimiento anticipativo.

Llegados a este punto, teniendo como referencia el análisis realizado por Rafael Jiménez Villalonga, en Global Strategy[5], sobre los tipos de inteligencia, esta, en virtud de su finalidad, puede ser calificada como estratégica, operativa o táctica.

Inteligencia estratégica es aquella orientada al largo plazo, vinculada con la formulación de políticas generales, planes de alto nivel y objetivos fundamentales de una organización o Estado, entre la que se incluye la seguridad nacional. En el contexto de la seguridad nacional, la inteligencia estratégica suministra a la alta dirección del Estado apreciaciones sobre el entorno global, identificando actores, tendencias, riesgos emergentes y oportunidades que puedan afectarlos. Dado su carácter anticipativo, está muy ligada a la prospectiva. En el ámbito empresarial, la inteligencia

[5] Vid. https://global-strategy.org/tipos-de-inteligencia/

estratégica apoya a la alta dirección de la empresa (en la definición de su estrategia corporativa de largo plazo)[6].

La inteligencia operativa ocupa el eslabón intermedio entre la formulación estratégica y la acción inmediata. Su cometido es traducir la orientación estratégica en planes con un horizonte de medio plazo, proporcionando a los niveles intermedios el conocimiento necesario para diseñar, sincronizar y evaluar operaciones en un ámbito determinado.

De esta forma, se asegura su alineación con los objetivos estratégicos y su producto debe integrar indicadores, riesgos y cursos de acción con métricas de desempeño[7].

Para finalizar, la inteligencia táctica se asocia al corto plazo y al día a día de las diferentes áreas, proporciona alertas y apoyos informativos muy concretos para decisiones inmediatas, normalmente a mandos de unidad y equipos operativos.

Es importante destacar que estos tres niveles forman un continuo: la inteligencia estratégica marca la dirección general, la operativa traduce esa dirección en planes y coordina los medios, y la táctica ejecuta acciones concretas informadas por inteligencia de detalle. Cada una atendiendo a diferentes escalones de decisión[8].

En definitiva, la distinción entre inteligencia estratégica, operativa y táctica resulta útil para asegurar que cada decisor recibe el tipo de inteligencia adecuado a sus necesidades, garantizando así la eficacia de un sistema global de inteligencia[9].

Por otro lado, existen muchas tipologías de inteligencia según la materia a tratar, en el caso de esta monografía, al versar sobre el entorno económico, se tratará de definir la inteligencia económica.

---

[6] Se especializa en analizar el macroentorno competitivo y económico, previendo escenarios futuros, movimientos de competidores, cambios tecnológicos o regulatorios, de modo que la empresa pueda orientar sus decisiones estratégicas informadas sobre posibles amenazas y oportunidades de negocio.

[7] La Estrategia Nacional contra el Crimen Organizado y la Delincuencia Grave 2025 inscribe explícitamente esta capa en el diseño de la respuesta pública, al exigir la integración de inteligencia estratégica y operativa como base de prevención, investigación y análisis frente a redes delictivas, lo que confirma la importancia estructural en la planificación de políticas y campañas.

[8] Alta dirección política, mandos intermedios ministeriales o fuerzas de seguridad, y unidades ejecutoras respectivamente.

[9] En esta monografía, la inteligencia irá vinculada a alguno de estos niveles según el contexto, siendo siempre igual de relevante.

La inteligencia económica (IE) se ha consolidado como una disciplina específica, con rasgos que la diferencian de otras modalidades afines como la inteligencia competitiva, la inteligencia empresarial, o las prácticas de *Big Data* y analítica de datos.

Una definición clásica, contenido en el Glosario de Inteligencia publicado por el Ministerio de Defensa de España, en 2007, describe la inteligencia económica como

> «el tipo de inteligencia 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».

La tradición francesa consolidó la IE en los años noventa con el Rapport Martre (1994) (Informe de Henri Martre), que la sitúa como la gestión estratégica de la información económica al servicio de la competitividad empresarial y del interés nacional, en un contexto de globalización y «guerra económica» no militar, pretendiendo coordinar la vigilancia, la protección del patrimonio informacional/tecnológico y la influencia (capacidad de proyectar normas y estándares) como función pública y de mantenimiento y desarrollo del ecosistema (Estado-empresa-territorios).

El «référentiel de formation en intelligence économique»[10], promovido por Alain Juillet[11], con el objeto de establecer los contenidos y pilares fundamentales para la formación de inteligencia económica en Francia, con un enfoque estratégico y operacional, formula una definición muy citada: la IE consiste en la gestión eficaz y la protección de la información estratégica por todo actor económico, con triple finalidad competitividad–seguridad–influencia.

Nicolas Moinet[12] enfatiza la IE como «dinámica colectiva» que busca agilidad mediante el uso estratégico de la información, reuniendo vigilancia, seguridad e influencia como campos operativos interdependientes.

[10] Referencia de formación en inteligencia económica.

[11] Fue nombrado en diciembre de 2003 «Haut responsable chargé de l'intelligence économique» (Alto Responsable para la Inteligencia Económica) por el primer ministro francés.

[12] Catedrático en la Université de Poitiers y figura destacada en la formación académica de inteligencia económica en Francia. Cofundador del Observatoire International de l'Intelligence Économique (OIIE).

Reino Unido ha tendido a integrar la IE en la noción más amplia de *national security intelligence*, centrada en la protección de intereses nacionales y financieros, en línea con las *UK National Security Strategies*. Existe un fuerte vínculo con la protección contra el espionaje económico y la seguridad corporativa.

Alemania mantiene un modelo de IE que asocia la *Wirtschaftsschutz* (protección económica) y la *Industrieschutz* (protección industrial) a la contrainteligencia empresarial y la seguridad industrial. El *Bundesamt für Verfassungsschutz* (BfV)[13] ha señalado en varios informes la relevancia de la inteligencia económica para la protección frente al espionaje industrial y tecnológico.

China ha desarrollado un modelo de inteligencia estratégica con un fuerte componente estatal, donde la IE forma parte de su expansión global y del control de sectores críticos. El concepto de «guerra económica» está explícitamente presente, con un uso instrumental del espionaje tecnológico y comercial.

En la práctica empresarial anglosajona, se distinguen dos planos, la inteligencia competitiva, (*Competitive Intelligence*, CI), definida como el proceso ético y sistemático de recogida y análisis sobre competidores, mercados y entorno para reducir el riesgo estratégico y anticipar actuaciones, apoyando las decisiones de la máxima dirección, y la inteligencia de negocios (*Business Intelligence*, BI), entendida como el conjunto de tecnologías y aplicaciones para explotar datos internos de la corporación (operativos/financieros/comerciales), así como producir cuadros de mando con informes analíticos relevantes para la toma de decisiones táctico-operativas[14].

Finalmente, es importante distinguir la IE, y sus variantes mencionadas, de conceptos como *Big Data* y la analítica de datos. *Big Data* alude al conjunto de tecnologías y metodologías capaces de extraer, almacenar y procesar volúmenes masivos de datos, a gran velocidad y con gran variedad de formatos, para extraer

[13] Oficina Federal para la protección de la Constitución.

[14] De esta forma, la inteligencia de negocios explota, principalmente, datos generados por la actividad interna (ventas, clientes, procesos, etc.), aplicando técnicas de minería de datos, análisis estadístico y visualización para obtener conocimientos accionables sobre el desempeño y las eficiencias o ineficiencias de la organización. A diferencia de la inteligencia competitiva, que mira al entorno externo, la BI mira hacia adentro, aunque ambas confluyen en proporcionar información de calidad para la estrategia empresarial. De hecho, suele englobarse a veces todo este espectro bajo el término amplio de inteligencia empresarial, entendiéndola como la inteligencia orientada a la toma de decisiones en la empresa en todos sus niveles (estratégico, táctico y operativo).

de ellos información útil. Sin embargo, el *Big Data* por sí mismo opera fundamentalmente en el plano de los datos e información, por lo que no supone de forma automática la generación de inteligencia en sentido estricto.

En relación con todo lo anterior, se infiere que la IE pública integra vigilancia, protección e influencia para salvaguardar los intereses nacionales y apoyar políticas; la IE empresarial converge con CI+BI para sostener la ventaja competitiva, mientras que el *Big Data* aporta capacidad.

Con base en ello, en este trabajo se entenderá por IE el producto dimanante de un proceso sistemático y legal de recolección, análisis, elaboración, protección y difusión de conocimiento accionable sobre factores, actores y dinámicas económicas (internas y externas) que afectan a la seguridad, a los intereses económicos legítimos (nacionales, sectoriales o corporativos), con participación público-privada, orientado a la toma de decisiones en tres niveles (estratégico, operativo y táctico).

En este sentido, la ESN-2021 incorpora un enfoque anticipatorio y de alerta temprana basado en el análisis de hechos y de datos objetivos, plenamente coherente con una IE de orientación pública que apoya la seguridad económica y la gestión de riesgos interdependientes[15].

En el ámbito de la Unión Europea, el EU SOCTA 2025 constituye la evaluación *intelligence-driven* de las amenazas de delincuencia grave y organizada con repercusión económica y sistémica. Sus conclusiones sirven de base para la definición de las prioridades del ciclo político-operativo de la Plataforma Multidisciplinar Europea contra las Amenazas Criminales (EMPACT) 2026-2029, aprobadas por el Consejo.

2.2 Actores que conforman el sistema económico

Con el fin de profundizar en la incidencia de lo económico, y, en consecuencia, la incidencia de la IE en la seguridad se considera necesario identificar los principales actores económicos y como interactúan entre ellos.

[15] En este mismo sentido, la Estrategia Nacional contra el Crimen Organizado y la Delincuencia Grave (ENCODG) 2025 (aprobada por el CSN y publicada por Orden PJC/846/2025), estrategia de segundo nivel, refuerza el eje de inteligencia como prevención, anticipación y neutralización de la economía del crimen, es decir, una IE pública aplicada a riesgos económico-criminales.

Este conocimiento posibilitará la detección de entidades generadoras de datos o información económico-financiera, a partir de los cuales se posibilita la elaboración de inteligencia económica y, en este marco, la identificación de nuevos ámbitos de aplicación de esa inteligencia en la lucha contra el crimen organizado y grave.

Por todo ello, se procederá a realizar una definición de los actores desde una perspectiva global, para después exponer otro listado asociado al ámbito nacional. Pues, según lo ya expuesto, lo internacional incide de manera significativa en lo local.

Desde una perspectiva global, los principales actores estarían incluidos en la siguiente categorización:

- Estados nacionales: establecen sus propias políticas económicas y de seguridad, con el fin de proteger sus intereses. Fundamentalmente, interactúan a través de acuerdos bilaterales o multilaterales, así como aplicando medidas proteccionistas de manera unilateral.
- Organizaciones supranacionales: la más representativa es la Unión Europea, aunque existen otras con un menor grado de integración supranacional o institucionalización, de este modo, se pueden incluir Mercado Común del Sur (MERCOSUR), Asociación de Naciones del Sudeste Asiático (ASEAN), UA o el tratado entre México, EE. UU. y Canadá (USMCA/T-MEC), todas ellas con un marcado carácter económico.

Estas organizaciones actúan de manera multidimensional y de forma asimétrica, llevando a cabo funciones de representación ante determinados organismos, facilitando el comercio y la inversión (tanto privada como pública), así como, posicionándose estratégicamente en los continuos reequilibrios del orden mundial. Todo ello, lo realizan de manera integrada con otros niveles de gobernanza y con los diversos tipos de actores.

- Organizaciones internacionales: estas instituciones, como el FMI, la ONU, el Banco Mundial (BM) o la OMC, facilitan la cooperación y el entendimiento en distintos ámbitos, fundamentalmente en el económico, posibilitando la resolución de conflictos en el marco de regulaciones aceptadas por los diferentes intervinientes, financiando o subvencionando, incluso, distintas iniciativas de desarrollo social y económico.
- Corporaciones multinacionales: actualmente, constituyen el motor comercial y de inversión del sistema económico global, lo que se proyecta en una gran influencia en dicho sistema.

- Foros de gobernanza informal o clubes de poder internacionales: en este nivel, se deben destacar el G-20, G-8, G-77 o los denominados BRICS: Brasil, Rusia, India, China, Sudáfrica. Aunque son estructuras no institucionalizadas, poseen una gran capacidad de influencia en el sistema económico global[16].
- *Think Tanks* y universidades: su actividad principal es la generación de conocimiento, pudiendo realizar análisis prospectivos y, consecuentemente, influir en las políticas estratégicas y, entre ellas, las económicas. Igualmente, interactúan con los estados y las corporaciones mediante informes estratégicos, asesorías o formación especializada.
- Actores no estatales: en esta categoría se sitúan las organizaciones no gubernamentales (ONG), sindicatos, los diversos grupos de interés y todos aquellos dimanantes de una sociedad civil organizada. De este modo, estos grupos ejercen su influencia sobre la gobernanza económica global mediante la presión social, incidencia en la Administración Pública y demandas de responsabilidad estatales y corporativas.

Este conjunto de actores, los intereses de estos y la actividad que desarrollan para alcanzarlos, configuran una arquitectura económica mundial extremadamente compleja, densa y, en cierta medida, estructurada. En este marco, se genera un orden económico híbrido, donde lo informal coexiste con lo formal, lo que amplía el rango de escenarios futuros posibles.

Si se centra el foco en España, los principales actores son los siguientes:

- Administración Pública.
- Organizaciones internacionales y supranacionales.
- Grandes empresas y pequeñas y medianas empresas (pymes).
- *Think Tanks*, universidades y centros tecnológicos.
- Actores no estatales y sociedad civil organizada.

[16] En este sentido, actúan como espacios de concertación política, derivando en una coordinación macroeconómica y en el establecimiento de agendas estratégicas de los distintos actores. Complementan a las organizaciones formales, maximizando su estructura no institucional e intergubernamental para conseguir un entendimiento político en escenarios complejos, adoptando decisiones rápidas y flexibles.

2.2.1 Administración Pública

Las administraciones públicas españolas se configuran, básicamente, en tres niveles: estatal (Administración General del Estado), autonómico (comunidades autónomas)[17] y local/municipal (ayuntamientos)[18].

El nivel estatal es el que aglutina las competencias más críticas, ostentando atribuciones exclusivas en fiscalidad (salvo excepciones), comercio exterior, seguridad económica, política monetaria (delegada en el BCE) y regulación financiera.

En base a ellas, articula la seguridad económica en seis ejes: la gestión de los sectores estratégicos a través de la Sociedad Estatal de Participaciones Industriales (SEPI), el control de la inversión extranjera directa (IED/FDI) en sectores sensibles, la supervisión financiera (BdE, CNMV, Tesoro) integrada en el marco europeo, la prevención de prácticas de blanqueo de capitales y financiación del terrorismo (PBC/FT) con el Servicio Ejecutivo de la Comisión de Prevención del Blanqueo de Capitales e Infracciones Monetarias (SEPBLAC) como Unidad de Inteligencia Financiera (UIF) nacional, la gestión de la ciberseguridad y el aseguramiento de las infraestructuras críticas (Centro Nacional de Protección de Infraestructuras Críticas (CNPIC), Centro Criptológico Nacional – Computer Emergency Response Team (CCN-CERT), Instituto Nacional de Ciberseguridad (INCIBE) y Oficina de Coordinación de Ciberseguridad (OCC)) y la regulación de los mercados estratégicos (CNMC y ministerios competentes).

El nivel autonómico también ejerce funciones económicas relevantes en un modelo multinivel y asimétrico [régimen común, foral y Régimen Económico y Fiscal (REF)], gestiona fondos UE y promueve el desarrollo mediante agencias y clústeres público-privados.

---

17 También, se considera un nivel intermedio, entre el autonómico y el local, constituido por las diputaciones provinciales (en los territorios de régimen común), los cabildos insulares, uno por isla en Canarias, los consells insulars, uno por isla mayor (Mallorca, Menorca e Ibiza) en Islas Baleares y las diputaciones forales del País Vasco, una por provincia. En Navarra, y en el resto de las comunidades uniprovinciales, no existen diputaciones, asumiendo sus funciones la comunidad foral o la comunidad del régimen común, respectivamente.
Las estructuras intermedias (diputaciones, cabildos, consells) coordinan y canalizan inversiones, mientras que las diputaciones forales disponen de una amplia autonomía tributaria y capacidad de política económica.

18 En las ciudades autónomas, Ceuta y Melilla, el ayuntamiento y el órgano autonómico están fusionados en una única institución: la ciudad autónoma.

Asimismo, el nivel local aporta fiscalidad propia, urbanismo y promoción económica, con un impacto significativo por número de municipios y el peso de grandes ciudades.

Todo ello refleja un panorama de la gestión económica multinivel que conjunta la complementariedad y una complejidad vinculada a una correspondencia asimétrica de competencias.

Los distintos niveles, en el marco económico, financiero y fiscal, se coordinan y cooperan a través de distintos órganos y procedimientos formales, en virtud de lo dispuesto en el artículo 103.1 de la Constitución española (CE) y los artículos 2.1.b y 3 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.

Así, el nivel estatal se relaciona con el autonómico, fundamentalmente, a través del Consejo de Política Fiscal y Financiera (CPFF)[19], conferencias sectoriales[20] y las Comisiones bilaterales Estado-CCAA[21].

2.2.2 Organizaciones internacionales y supranacionales

Las organizaciones que se podrían incluir en este apartado alcanzan un número muy elevado, precisamente por la enorme interacción mundial que ya se ha descrito entre los distintos actores intervinientes. En este sentido, se ha considerado que, para este estudio, lo adecuado es centrarse en la que mantiene una mayor influencia en el sistema económico español, la UE.

Se debe tener en cuenta que la CE prevé la cesión de competencias mediante ley orgánica en su artículo 93, así como la incorporación de tratados al derecho interno, según lo dispuesto en el artículo 96.

Según el artículo 2 del Tratado de Funcionamiento de la UE (TFUE), existen competencias exclusivas de la UE, recogidas en el artículo 3, competencias compartidas con los Estados miembros, artículo 4, y competencias de apoyo, artículo 6 del tratado.

Entre las competencias exclusivas se encuentran la unión aduanera, el establecimiento de las normas sobre competencia, la política monetaria (en los países de la zona euro) y la política

19 Órgano colegiado previsto en la Ley Orgánica 8/1980, de financiación de las CC. AA.

20 Previstas en el artículo 147 de la Ley 40/2015.

21 Dispuestas para las CC. AA. con estatutos reforzados o régimen especial (Cataluña, País Vasco, Navarra, Canarias).

comercial común. Respecto a las compartidas se pueden destacar el mercado interior, cohesión económica, redes transeuropeas, energía, medio ambiente y consumidores[22].

Resulta evidente, por tanto, que esta cesión competencial, total o parcial, condiciona la seguridad económica de España a la UE.

En el marco de la seguridad económica, la UE ejerce el cribado de inversiones extranjeras directas (FDI *screening*), Mecanismo Único de Supervisión (MUS), Mecanismo Único de Resolución (MUR) y el Sistema Europeo de Supervisión Financiera (SESF), regulado principalmente por el Reglamento (UE) n.º 1092/2010 del Parlamento Europeo y del Consejo, de 24 de noviembre de 2010.

La UE, además, posee instrumentos para proteger el mercado europeo como medidas *antidumping*, y antisubvenciones, el Reglamento de obstáculos al comercio y las medidas de salvaguardia[23].

2.2.3 Grandes empresas[24] y pymes

Las grandes corporaciones españolas, muchas agrupadas en el IBEX-35, son actores decisivos tanto por su capacidad de inversión, como por su influencia en la política económica y su papel como tractores del ecosistema empresarial.

Según la Asociación Valenciana de Empresarios (AVE), la aportación al Producto Interior Bruto (PIB) del conjunto de las empresas españolas fue en 2024 del 86,8 % del total[25]. De igual forma, la Dirección General de Apoyo a la Pequeña y Mediana Empresa

---

22 EUR-Lex, Reparto de competencias en la Unión Europea. Disponible en: https://eur-lex.europa.eu/ES/legal-content/summary/division-of-competences-within-the-european-union.html?utm_source [Consulta: 8 agosto 2025].

23 EUR-Lex, Política comercial UE. Disponible en: https://eur-lex.europa.eu/ES/legal-content/glossary/eu-trade-policy.html?utm_ [Consulta: 8 agosto 2025].

24 La Recomendación 2003/361/CE de la Comisión Europea clasifica como gran empresa a aquella que supera doscientos cincuenta empleados y presenta un volumen de negocios anual superior a cincuenta millones de euros o un balance general anual superior a 43 millones de euros.

Las corporaciones multinacionales (CMN) se definen doctrinalmente como aquellas entidades que poseen o controlan activos productivos en más de un país, operando bajo una estructura corporativa integrada, pero con filiales que actúan conforme a los marcos regulatorios propios de los territorios donde están ubicadas. UNCTAD (2023). World Investment Report 2023: Investing in Sustainable Energy for All. United Nations Conference on Trade and Development. Disponible en: https://unctad.org/wir [Consulta: 8 agosto 2025].

25 Asociación Valenciana de Empresarios (AVE), Barómetro del empresario, 2025. Disponible en: https://barometrodelempresario.es/ediciones/ [Consulta: 8 agosto 2025].

(DGEIPYME) indica que el valor añadido bruto (VAB)[26] de las grandes empresas en España era del 37,8 %, mientras que el de las pymes, incluido autónomos, es del 62,2 %, sin incluir a las financieras, según lo dispuesto en el informe emitido por la DGEIPYME «Marco Estratégico en Política de Pyme 2030», de 2019.

En el contexto español, las grandes empresas y corporaciones multinacionales (CMN) desempeñan un papel determinante en el producto interior bruto, el empleo y la balanza comercial, concentrando un volumen significativo de facturación y exportaciones[27] pese a representar un porcentaje reducido del total de sociedades registradas. En este sentido, constituyen un 55,6 % del volumen de las exportaciones[28].

A su vez, de acuerdo con la estadística de empresas según pertenencia a grupos elaborado por el Instituto Nacional de Estadística (INE), en 2022 se contabilizaron 5514 empresas residentes en España integradas en grupos multinacionales de matriz española (empresas controladoras con filiales en el extranjero) y 14 209 empresas pertenecientes a multinacionales extranjeras[29].

Las pymes representan el 99 % de las empresas existentes en España según la DGEIPYME, atendiendo a las referencias mostradas en párrafos anteriores. Paralelamente, mantienen más o menos el 66 % del empleo empresarial total.

Además, las pymes coadyuvan a la cohesión territorial, fijando población en territorios y reduciendo los desequilibrios regionales, a la diversificación productiva, favoreciendo la resiliencia económica frente a potenciales crisis, aplicando la innovación en proyectos con universidades y centros tecnológicos y aportan valor añadido al insertarse en las cadenas de suministros como proveedores especializados.

---

[26] Índice íntimamente ligado al PIB, según lo descrito por el Instituto Galego de Estadística: Definiciones. Economía. Disponible en: https://www.ige.gal/igebdt/esq.jsp?c=0307&idioma=es&ruta=definiciones/defcod.jsp?C=03070000 [Consulta: 8 agosto 2025].

[27] Subdirección General de Estudios y Prospección: El sector exterior en 2023. Disponible en: https://www.revistasice.com/index.php/SICE/article/view/7757 [Consulta: 8 agosto 2025].

[28] Ministerio de Economía, Comercio y Empresa: Informe de Evaluación a medio camino de la Estrategia de Internacionalización de la Economía Española 2017-2027. Disponible en: https://comercio.gob.es/es-es/estrategia_internacionalizacion/Documents/20231222-Evaluacion-EIEE-2017-27.pdf [Consulta: 9 agosto 2025].

[29] INE: Estadística de Empresas según Pertenencia a Grupos. Año 2022. Disponible en: https://ine.es/dyngs/Prensa/EEPG2022.htm. [Consulta: 8 agosto 2025].

Por otro lado, las Cámaras Oficiales de Comercio, Industria, Servicios y Navegación, reguladas por la Ley 4/2014, de 1 de abril, Básica de las Cámaras Oficiales de Comercio, Industria, Servicios y Navegación, actúan como agentes institucionales clave en el fortalecimiento de las pymes, favoreciendo la internacionalización, procurando la formación y la digitalización, apoyando la financiación y el emprendimiento, y elaborando inteligencia económica local, mediante la recopilación y la difusión de información sectorial y de mercado útil para la toma de decisiones empresariales, todo ello, en base a sus propias competencias.

2.2.4 Think tanks, universidades y centros tecnológicos

En el marco del sistema económico español, los *think tanks*, universidades y centros tecnológicos constituyen nodos esenciales para la generación, transferencia y aplicación de conocimiento, tanto en el plano nacional como internacional. Su actividad incide de forma directa en la competitividad, la innovación, en la toma de decisiones y la resiliencia del tejido productivo, y, de manera indirecta, en la seguridad económica del Estado.

- Think tanks

  En el contexto español, los *think tanks* actúan como plataformas de análisis e investigación que elaboran estudios prospectivos, informes de estados de situaciones concretas y propuestas de política pública.

  Según la clasificación del *Think Tanks and Civil Societies Program* de la Universidad de Pensilvania (2020)[30], España se sitúa en el puesto 17 mundial, por número de *think tanks*, reconociendo la relevancia internacional por parte del Real Instituto Elcano del Barcelona Centre for International Affairs (CIDOB) o la Fundación de Estudios de Economía Aplicada (FEDEA), que proporcionan análisis estratégicos en ámbitos como la geoeconomía, la política exterior o la economía industrial, entre otros.

- En el ámbito económico, su valor reside en la capacidad de generar IE y transferirla a las administraciones públicas, empresas y sociedad civil, contribuyendo a la formulación de políticas y a la anticipación de riesgos. Actuando, de este modo,

[30] The Lauder Institute, University of Pennsylvania: 2020 Global Go To Think Tank Index Report. Disponible en: https://repository.upenn.edu/bitstreams/8fa7709a-310d-43b2-bee6-94c49db23e41/download [Consulta: 10 de agosto 2025].

como puente entre el ámbito académico y la toma de decisiones políticas (McGann, 2020).

– Universidades

Según el Ministerio de Ciencias, Innovación y Universidades el impacto económico de las universidades públicas españolas en la economía se cifra en el 2,2 % del PIB[31]. Pero su aportación va mucho más allá.

Las universidades, públicas y privadas, desarrollan un papel estructural en la formación de capital humano altamente cualificado, en la investigación aplicada y en la cooperación universidad-empresa[32].

En el plano económico, los programas de transferencia tecnológica y de innovación abierta permiten a las universidades conectar con pymes y grandes empresas para impulsar la I+D+i, en coordinación con el sistema estatal de ciencia, tecnología e innovación regulado por la Ley 14/2011, de 1 de julio, de la Ciencia, la Tecnología y la Innovación.

Estos centros además generan IE a través de su actividad investigadora, formando también expertos en esta temática a través de formación especializada.

– Centros tecnológicos

Los centros tecnológicos españoles, agrupados en redes como Federación Española de Centros Tecnológicos (FEDIT) o Tecnalia en el País Vasco, constituyen entidades de apoyo a la innovación empresarial, proporcionando capacidades de investigación aplicada, desarrollo experimental y validación industrial.

Según el Plan Estatal de Investigación Científica, Técnica y de Innovación 2021-2027, estos centros son instrumentos clave para cumplir los objetivos de digitalización, transición

[31] Ministerio de Ciencias, Innovación y Universidades: Estudio de impacto económico de las universidades públicas españolas. Análisis territorializado para el año 202. Disponible en: https://www.ciencia.gob.es/Noticias/2023/junio/Las-universidades-publicas-espanolas-multiplican-por-5--cada-euro-invertido-en-ellas.html#:~:text=Las%20universidades%20p%C3%BAblicas%20espa%C3%B1olas%20multiplican%20por%205,la%20actividad%20de%20las%20universidades%20p%C3%BAblicas%20espa%C3%B1olas [Consulta: 10 agosto 2025].

[32] La Ley Orgánica 2/2023, de 22 de marzo, del Sistema Universitario (LOSU) establece, en su artículo 3, que la misión de las universidades incluye la transferencia, difusión y valorización del conocimiento para el desarrollo social y económico.

energética y fortalecimiento de la autonomía estratégica industrial. Su financiación combina aportaciones públicas (nacionales y europeas) y servicios de I+D+I contratados por empresas.

Desde una perspectiva de IE, estos actores contribuyen a detectar y analizar tendencias globales con capacidad de impactar en la economía española, transferir conocimiento y tecnología para fortalecer los distintos sectores estratégicos, aumentando la independencia tecnológica y sirviendo de enlace eficaz entre el sector público y privado.

2.2.5 Actores no estatales y sociedad civil organizada

Sindicatos, organizaciones empresariales como la Confederación Española de Organizaciones Empresariales (CEOE) y la Confederación Española de la Pequeña y Mediana Empresa (CEPYME), ONG sectoriales y asociaciones ambientales tienen una influencia creciente en la deliberación de políticas públicas.

Interactúan con el Estado mediante el diálogo social y con las empresas a través de la negociación colectiva y programas de responsabilidad social corporativa (RSC)[33].

Un ejemplo de participación en las políticas económicas de sindicatos, organizaciones empresariales y Administración es el Consejo Económico y Social, según lo dispuesto en la Ley 21/1991, de 17 de junio, por la que se crea el Consejo Económico y Social.

2.3 Generación de inteligencia económica por los distintos actores

De todo lo expuesto en el apartado anterior, se puede observar que la realidad del sistema económico español se vincula, de manera especial, a una estructura multinivel de gobernanza asimétrica que deriva en una red compleja de competencias. Estas competencias determinan la capacidad de acción de cada nivel.

Los distintos niveles interactúan, además, con los diferentes actores privados y no estatales, dependiendo de los intereses y competencias de cada uno de ellos.

[33] Observatorio de Responsabilidad Social Corporativa. Disponible en: https://observatoriorsc.org/ [Consulta: 10 agosto 2025].

Todo este sistema se complica al enmarcarlo, y en gran medida supeditarlo, al ámbito internacional. En este sentido, la cesión de soberanía a la UE, en materia económica, influye decisivamente en el sistema económico español, más aún si se atiende a la financiación de proyectos y concesión de subvenciones provenientes de la UE.

Esta influencia europea se intensifica al incorporar el hecho de que la UE es la zona prioritaria de las exportaciones e importaciones españolas, con un 61,8 % y 48,9 %, respectivamente[34], lo que evidencia que cualquier estrategia de seguridad económica debe estar alineada con la que desarrolle la UE.

También se aprecia, de la descripción de los diferentes actores, que, aunque existe una interacción entre todos los niveles (incluyendo el internacional), la coordinación y la cooperación del conjunto se vehiculiza, de manera referencial, a través de la Administración central. Este hecho es relevante para establecer fórmulas eficientes en la aplicación práctica del conocimiento, especialmente en el ámbito de la IE.

Una vez que se han definido los distintos actores se requiere conocer si generan IE o si su actividad posibilitase la generación de esta.

En primer lugar, en el marco internacional, se analizará la UE por resultar el ente supranacional con mayor incidencia en el sistema económico español.

2.3.1 Inteligencia económica en el marco de la UE

El ecosistema UE de inteligencia, y la económica en particular, se articula en torno a varias agencias u organismos propios.

Así el Centro de Inteligencia y situación de la UE (EU INTCEN) (parte civil de la SIAC), produce evaluaciones *all-source*[35] y comparte su análisis con la Comisión, las demás agencias europeas y con los Estados miembros.

[34] Informe Mensual de Comercio Exterior junio 2025. Ministerio de Industria, Comercio y Turismo. Disponible en: https://comercio.gob.es/ImportacionExportacion/Informes_Estadisticas/Historico_Informes/Mensuales/2025/2025-06_Informe_Mensual_Comercio_Exterior.pdf [Consulta: 11 agosto 2025].

[35] Producto de inteligencia resultante de la fusión y validación de información procedente de todas las disciplinas y canales disponibles, con el fin de reducir incertidumbre y orientar decisiones.

La Oficina Europea de Lucha contra el Fraude (OLAF) investiga administrativamente el fraude y la corrupción que afectan a los intereses financieros de la UE, generando inteligencia estratégica y operativa mediante distintos informes periódicos o información concreta con la que nutre causas judiciales y de manera referencial al European Public Prosecutor's Office (EPPO).

En el marco de la lucha contra falsificación/piratería, la oficina de Propiedad Intelectual de la Unión Europea (EUIPO)-Observatorio constituye una referencia internacional con el desarrollo de estudios y buenas prácticas.

Por otro lado, EUROPOL, que cuenta con un departamento específico dedicado al ámbito económico, el Centro Europeo de Delincuencia Financiera y Económica (EFECC), brinda apoyo operativo-analítico en delincuencia financiera/económica, incluyendo la trazabilidad de bienes ilícitos y su decomiso, coordinando la Asociación Público-Privada de Inteligencia Financiera de EUROPOL EFIPPP[36].

La generación de IE que realiza la UE, a través del sistema económico y de seguridad, evidencia una estructura cohesionada en aras de preservar una de las mayores fortalezas de la UE, su poder económico (Damro, 2012). Esta fortaleza le permite una significativa influencia en la gobernanza mundial (Bradford, 2015), en concordancia con los objetivos de la IE.

Por ello, la UE considera esencial mantener una seguridad económica eficaz, en un mundo cada vez más tensionado con una afectación significativa a las relaciones económicas, como ya se ha expuesto. Muestra de este compromiso se evidencia en la adopción de la «Estrategia europea de seguridad económica», de 20 de junio de 2023.

De esta manera, la IE es fundamental para la toma de decisiones que garantice la pretendida seguridad económica, en un ámbito internacional donde los elementos económicos pueden ser utilizados como instrumentos de presión, coerción o para acumular poder (Farrell y Newman, 2019).

También se observa como estos productos de inteligencia son empleados en la lucha contra actividades ilegales, tanto desde una perspectiva administrativa como penal. Configurándose la

[36] Es una red creada en 2017 para compartir información y coordinarse entre Europol, autoridades competentes (FIU, policía/investigación) y entidades financieras frente al blanqueo y el crimen financiero/económico. Su secretaría está en el EFECC (Europol).

cooperación entre los Estados miembros, las propias instituciones de la EU, las empresas e, incluso, países terceros, como un elemento determinante para la utilización eficiente de la referida inteligencia. En tal sentido, la UE ha normalizado los mecanismos de cooperación.

2.3.2 Generación de inteligencia económica en el marco español

La producción de inteligencia no deriva de una única entidad, sino de una comunidad. Esta comunidad de inteligencia puede conceptualizarse como una federación funcional de organismos ejecutivos que, aunque cooperan y a veces integran esfuerzos, sirven a decisores distintos y operan bajo líneas de autoridad diferentes. Este entramado se va configurando a través de un proceso transformacional, no derivado de un diseño previo, y que combina especialización y coordinación para producir inteligencia al servicio de la decisión política (Lowenthal, 2012).

En el ámbito español, la comunidad de inteligencia española se correspondería con un sistema compuesto por los servicios de inteligencia e información del Estado y por los distintos órganos de coordinación, orientado a evitar la dispersión de esfuerzos y a garantizar eficiencia y eficacia en la generación e intercambio de inteligencia para la decisión política en el contexto de la seguridad nacional, entendiendo el término seguridad en una acepción amplía (Rosales Pardo, 2005).

La Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia, recoge la existencia de una comunidad de inteligencia, mediante su artículo 6 «La Comisión Delegada del Gobierno para Asuntos de Inteligencia velará por la adecuada coordinación de todos los servicios de información e inteligencia del Estado para la formación de una comunidad de inteligencia».

Se le encomienda, por tanto, a esta comisión delegada la coordinación de los diferentes actores de inteligencia e información, integrantes de la comunidad. Así como, proponer al presidente del Gobierno los objetivos anuales para el CNI, que se materializarán en la Directiva de inteligencia, de frecuencia anual y de carácter secreto.

Sin embargo, la comunidad de inteligencia en España no está definida. En virtud de lo dispuesto en el artículo 6.1 y 6. 4c) de la Ley 11/2002, de 6 de mayo y del artículo 4 del Real Decreto 1/2024, de 9 de enero, la comunidad se constreñiría a

la Administración civil y militar, de la Administración General del Estado:

- CNI.
- Centro de Inteligencia de las FAS (CIFAS).
- Servicios de información de Interior:
    - Comisaría General de Información (Policía Nacional).
    - Jefatura de Información (Guardia Civil).
- Centro de Inteligencia contra el Terrorismo y el Crimen Organizado (CITCO).
- Centro Criptológico Nacional (CCN).
- INCIBE.
- SEPBLAC.
- AEAT:
    - Servicio de Vigilancia Aduanera (SVA).
    - Oficina Nacional de Investigación del Fraude (ONIF).
    - Oficina Nacional de Investigación de Aduanas e Impuestos Especiales (ONI).

Sin embargo, en el presente estudio se adopta una conceptualización ampliada de la comunidad de inteligencia, sustentada en un enfoque sistémico, holístico e integrado, que incluye no solo a las administraciones con competencias tradicionales en seguridad y defensa, sino también a otras administraciones públicas, a la sociedad civil organizada y al sector empresarial (Arcos y Antón, 2010).

En sintonía con lo expuesto, la generación de IE en España comprende un ecosistema amplio de actores públicos, privados y sociales, enmarcado por estrategias nacionales y normativas específicas.

Siguiendo un enfoque similar al de la UE, España ha ido reconociendo la IE como herramienta clave para la seguridad nacional y la competitividad (Díaz Matey, 2016). De hecho, la ESN 2021 identifica la seguridad económica como un pilar esencial, destacando en los Informes Anuales de Seguridad Nacional (IASN) que los riesgos económicos (inestabilidad financiera, fraude, blanqueo, etc.) socaban el bienestar y la confianza en las instituciones.

Consecuentemente, resulta esencial impulsar iniciativas para dotar al país de estructuras y mecanismos de IE que permitan anticipar riesgos y aprovechar oportunidades en un entorno global competitivo (Davara Rodríguez, 2015).

3 La delincuencia organizada y grave y su afectación a los intereses económicos

Como se ha ido poniendo de manifiesto a lo largo de este documento, la estrecha relación económica entre la UE y España, sumado al hecho de ser un Estado miembro de este organismo supranacional, ocasiona que las políticas económicas de la UE influyan notablemente en las españolas. Esta circunstancia, determina que la seguridad económica, en concordancia con los postulados de la UE, se configure como una pieza fundamental en la seguridad nacional.

En este sentido, ambas estrategias coinciden en identificar al crimen organizado y grave como una de las amenazas que pone en riesgo al sistema económico. En este escenario, conviene determinar qué ámbitos delictivos tienen la capacidad de menoscabar en mayor medida el sistema económico descrito.

Los Informes SOCTA de Europol (2021, 2025) confirman que la delincuencia organizada en Europa se configura de forma policéntrica, generando un sistema en el que se distribuyen numerosas redes y actores que interactúan entre sí, en el marco de los distintos mercados criminales.

Por otro lado, se ha determinado que más del 80 % de las redes criminales activas en la UE utilizan estructuras empresariales legales en sus operaciones (SOCTA, 2025), lo que pone de relieve una penetración sistemática en sectores regulados e infraestructuras críticas, como puertos y plataformas logísticas.

De este modo, el Informe sobre delincuencia financiera y económica de EUROPOL (2023) subraya que los sistemas financieros europeos y los profesionales facilitadores se encuentran en el corazón de la economía criminal.

Estos facilitadores, frecuentemente, se erigen en conectores de varias redes criminales a través del denominado *crime as a service*, siendo contratados sus servicios por redes diferentes. A partir de este diagnóstico, el EFECC recomienda integrar la inteligencia financiera y criminal desde las fases iniciales de las

investigaciones, con el fin de impedir la entrada de fondos ilícitos en la economía formal y aumentar las posibilidades de recuperación de activos.

En síntesis, la UE ha institucionalizado un enfoque en el que la IE y financiera ocupa una posición central para identificar, anticipar y neutralizar las formas más lesivas de criminalidad organizada.

Con la Estrategia Española de Seguridad (EES-2011), España comenzó a integrar de forma expresa los riesgos económicos y financieros en su agenda de seguridad, incluyendo la fragilidad del sistema financiero, el fraude fiscal, la corrupción y el blanqueo de capitales, reconociendo, asimismo, la función de la inteligencia estratégica para prevenir y responder a estas amenazas.

De este modo, anunció la creación de un Sistema de Inteligencia Económica (SIE) para prevenir y detectar acciones contrarias a los intereses económicos, financieros, comerciales y tecnológicos en los distintos sectores estratégicos españoles, coadyuvando al fortalecimiento de la seguridad nacional. Igualmente, ponía en valor y reconocía la necesidad de potenciar la inteligencia relacionada con la lucha contra el crimen organizado.

Asimismo, evidencia la conexión entre la amenaza que supone la inseguridad económica y el crimen organizado, en virtud de lo cual, considera esencial una mayor intensidad en la investigación criminal económica y su enfoque en el blanqueo de capitales procedente del crimen organizado, desarrollando unidades especializadas.

En relación con el mantenimiento de la seguridad económica y el correcto funcionamiento del sistema económico, subraya la necesidad de generar inteligencia económica y de luchar contra el fraude fiscal, el blanqueo de capitales, la corrupción, los paraísos fiscales y los distintos tráficos ilícitos que ponen en peligro la estabilidad económica y la financiación de las instituciones. En este sentido, destaca la importancia de la inteligencia estratégica para luchar contra el crimen organizado.

La ESN 2021 resalta que el fin económico del crimen organizado y la delincuencia grave socaban la seguridad nacional, utilizando estructuras legales y criptomonedas para opacar sus negocios ilícitos, resultando especialmente desestabilizador el contrabando, el cibercrimen, el tráfico de drogas, de armas y de especies silvestres y la corrupción.

Concretamente, ponen en riesgo la seguridad económica «el fraude, la evasión fiscal, la corrupción, el blanqueo de capitales y el uso indebido de los fondos procedentes de subvenciones y contratos públicos», generando, además, desafección social a las instituciones gubernamentales.

De esta forma, explicita los riesgos económicos sistémicos, reseñando la necesidad de la cooperación interinstitucional para gestionarlos eficazmente.

La ENCODG 2019-2023 pone de manifiesto la amenaza que supone el crimen organizado y la delincuencia grave para la seguridad nacional, desestabilizando y perturbando la economía nacional mediante el blanqueo de capitales, la creación de mercados paralelos o distorsionando determinados sectores productivos a través del ejercicio de la competencia desleal, utilizando inyecciones de capital provenientes de actividades ilícitas o eludiendo fraudulentamente cargas fiscales[37].

Entre sus ejes se encuentran la explotación de inteligencia económico-financiera, el impulso de investigaciones patrimoniales y la recuperación de activos.

La ENCODG 2025 profundiza en este modelo mediante el concepto de «anticipación operativa», es decir, el uso de análisis prospectivo, *Big Data* e IA para detectar, en fases tempranas, fenómenos de fraude, blanqueo y ciberamenazas financieras. Asimismo, prioriza la cooperación estructurada interinstitucional y público-privada.

Este deterioro del sistema económico[38], como apuntan los diferentes documentos estratégicos, se puede llevar a cabo de múltiples formas, a través de la infiltración en mercados legales (Savona y Riccardi, 2015), de la corrupción y de la extorsión minorizando la inversión (Blackburn *et al*., 2017), de la inyección de dinero sucio horadando la competencia (UNICRI, 2016) o generando burbujas especulativas, desviando capital de sectores productivos y aumentando la vulnerabilidad financiera.

[37] Esta estrategia también pone el foco en el fraude fiscal, en los delitos contra la propiedad intelectual e industrial, así como en la ciberdelincuencia aplicada a las finanzas.

[38] El referido informe Shadow Money de Europol (2021) estima que hasta 1,5 billones de euros perteneciente a ciudadanos europeos se sitúan ocultos en jurisdicciones offshore, es decir, depositados en territorios o centros financieros ubicados fuera del país de residencia, caracterizados por una fiscalidad reducida y por elevados niveles de opacidad.

Según el informe «VAT gap in the EU: 2024 report»[39] (European Commission, CASE *et al*., 2024), en 2022, la diferencia entre los ingresos teóricos de IVA y la recaudación efectiva fue del 7 % en la UE (89,3 mil millones de euros). Mientras que, en España, se dejaron de recaudar 4443 millones de euros (4,6 %). Destacando, asimismo, que el fraude del impuesto es el motor de esta diferencia.

Por otro lado, el Consejo de la UE publicó, en 2023, que se han detectado en el sistema financiero de la UE actividades y transacciones sospechosas por una horquilla de 117 000 y 210 000 millones de euros, así como 1500 millones de euros en movimientos de criptomonedas en los mercados de la web oscura. En este marco, determina que el 70 % de las redes delictivas activas en la UE emplea alguna forma de blanqueo de capitales para financiar sus operaciones y ocultar sus activos[40].

3.1 Ámbitos delictivos con mayor incidencia económica

Poniendo en común las distintas estrategias referidas, las entidades y organismos generadores de información e IE y la descripción del sistema económico, junto con el referido impacto que la delincuencia organizada y grave realiza en los intereses económicos de la UE y de España, se desprende una serie de ámbitos delictivos asociados a una mayor incidencia negativa en la seguridad económica.

La convergencia de las estrategias española y europea identifica, con notable consistencia temporal, un núcleo de criminalidad de alto impacto económico compuesto por:

1. Blanqueo de capitales.
2. Fraude Fiscal.
3. Cibercriminalidad económica.
4. Economía derivada del tráfico de drogas.

---

[39] El *VAT compliance gap* es la diferencia entre la *VAT Total Tax Liability* (VTTL) (la obligación teórica de IVA calculada con el método «top-down») y los ingresos efectivos de IVA registrados en contabilidad nacional (base devengo). Es decir, mide lo que no se recauda por incumplimiento, fraude, etc.

[40] Consejo de la UE. Análisis. ¿Qué es el blanqueo de capitales? Disponible en: https://www.consilium.europa.eu/es/infographics/anti-money-laundering/#:~:text=El%20blanqueo%20de%20capitales%20en,la%20econom%C3%ADa%20de%20la%20UE . [Consulta: 26 agosto 2025].

5 Delitos contra el mercado y la propiedad intelectual/ industrial.

6 Criminalidad medioambiental.

7 Trata de seres humanos.

Esta priorización emerge de la serie EU-SOCTA de EUROPOL (2013, 2017, 2021 y 2025) estando alineadas con las ESN (2011, 2013, 2017 y 2021) y con las ENCO (2019 y 2025).

Este núcleo representa la perspectiva económica de las prioridades[41] definidas en el EMPACT 2026-2029[42].

En la determinación de estas prioridades por el Consejo de la UE, se ha tenido en cuenta la creciente desestabilización que provoca en la sociedad la delincuencia organizada y grave, haciendo uso, en numerosos casos, de la violencia o la corrupción, así como su rápida adaptación al empleo de la AI y a las nuevas tecnologías.

3.1.1 Blanqueo de capitales

Es el soporte de la delincuencia organizada y grave actual, a través de esta práctica delictiva oculta, recoloca, invierte y disfruta de los bienes ilícitos conseguidos. Por ello, se erige en el objetivo principal para erradicar la criminalidad organizada y grave (EUROJUST, 2022), afectando a sus reservas y a su financiación (Balas Dávila, 2023).

Como ya se ha referido, el blanqueo de capitales desestabiliza y perturba la economía, creando un mercado paralelo que reduce la productividad, destruye la competencia e inhibe la actividad empresarial.

---

41 Identificar y desarticular las redes delictivas y las personas que representan una mayor amenaza.

Abordar los delitos que aumentan con mayor rapidez en el ámbito digital: ciberataques, explotación sexual de menores en línea y sistemas de fraude en línea;

Luchar contra el tráfico de drogas.

Luchar contra el tráfico ilícito de migrantes y la trata de seres humanos.

Luchar contra la delincuencia relacionada con armas de fuego y explosivos.

Desarticular redes implicadas en delitos contra el medio ambiente.

Luchar contra los delitos económicos y financieros, como el fraude del IVA y los delitos en materia de propiedad intelectual e industrial.

42 Conclusiones del Consejo sobre la mejora de la EMPACT y las prioridades de la UE en materia de lucha contra delincuencia para el próximo ciclo de la EMPACT 2026-2029, 13.6.2025. Disponible en: https://data.consilium.europa.eu/doc/document/ST-9397-2025-INIT/en/pdf [Consulta: 26 agosto 2025].

En base a ello, la ENCODG 2019-2023 ya marcaba siete líneas de acción entre las que se encontraba la de potenciar la inteligencia económica-financiera, mejorando su producción y la colaboración interagencias[43]. Así como fomentar la colaboración público-privada y la elaboración de un plan estratégico de lucha contra el enriquecimiento ilícito de las organizaciones criminales y los delincuentes.

La UE, consciente del daño económico de esta modalidad delictiva[44] y con el fin de proteger su mayor fortaleza como potencia económica, ha sido muy prolija en iniciativas y generación de normativa que sirva, de manera eficiente, en la lucha contra el BC. En este sentido y como hito destacado de los últimos años, la UE aprobó en 2024 el paquete contra el blanqueo de capitales[45], en el que se incluye la creación de la Autoridad Europea contra el Blanqueo de Capitales (AMLA).

EUROPOL insiste en que convertir la inteligencia financiera en impacto operativo (embargos, decomisos, cierres de canales de blanqueo) es clave para vaciar de recursos a las redes criminales y proteger la economía legal.

El SEPBLAC, entre 2022 y 2023, ha recibido 13 800 comunicaciones, ha atendido 2.300 solicitudes de información, ha analizado 22 000 millones de euros asociadas a distintas operativas sospechosas y ha realizado más de 10 000 informes de inteligencia, los cuales han sido remitidos a los organismos pertinentes (SEPBLAC, 2024).

3.1.2 Fraude fiscal

El fraude fiscal y, en particular, el fraude al Impuesto sobre el IVA mediante el esquema de *Missing Trader Intra-Community*

[43] AEAT, Seguridad Social, Oficina de recuperación y gestión de activos (ORGA), entidades financieras, SEPBLAC, Registro de la propiedad, Registro Mercantil, Registro de bienes muebles e inmuebles, ayuntamientos, compañías de suministro, autoridades policiales, etc.

[44] Se debe tener en cuenta que el número de casos vinculados únicamente al blanqueo de capitales monitorizados por EUROJUST solo es superado por los que representan los delitos económicos (excluyendo el blanqueo de capitales) y el tráfico de drogas (EUROJUST, 2025).

[45] Consta de tres normas: Reglamento (UE) 2024/1620 (AMLA), Reglamento (UE) 2024/1624 (reglamento de libro único) y Directiva (UE) 2024/1640 (mecanismos nacionales).

(MTIC)[46] o procedimientos defraudatorios similares, representan, desde hace varias décadas, una de las amenazas económicas más graves para la UE y España, al constituir una fuente recurrente de pérdida de ingresos públicos y representar un mecanismo asociado a redes delictivas organizadas, lo cual multiplica su capacidad de daño[47].

Evaluaciones recientes (Europol, 2025) reafirman que la amenaza persiste y que las redes usan estructuras societarias complejas y cadenas logísticas para ocultar el flujo de bienes y facturación, cuantificando el impacto del fraude de IVA en varias decenas de miles de millones de euros anuales.

En este sentido, prácticas como el MTIC abaratan artificialmente el producto que ofrecen los operadores fraudulentos frente a los ofertados por las empresas cumplidoras, expulsando a estas del mercado, en un efecto cascada, propiciando ciclos de inversión de baja productividad al canalizar beneficios ilícitos hacia actividades pantalla (UNICRI, 2016).

El SEPBLAC destaca la importancia de las tramas de defraudación de IVA, asociadas a organizaciones criminales, exponiendo, como caso paradigmático, el sector de la distribución de hidrocarburos por su altos importes, su impacto recaudatorio y su capacidad de blanqueo (SEPBLAC, 2024), lo que suponen, igualmente, una afectación grave al mercado.

La EPPO reportó en su Informe Anual 2024 que mantenían 2666 investigaciones activas, principalmente vinculadas a la delincuencia organizada. El perjuicio a los intereses financieros de estas investigaciones se ha estimado en más de 24 800 millones de euros. En este marco, el fraude de IVA representaba el 53 %, unos 13 150 millones de euros, indicador de la relevancia de este fraude en la criminalidad económica que afecta al presupuesto de la UE y a los LEA (European Public Prosecutor's Office, 2025).

[46] El fraude asociado al MTIC consiste en que una empresa adquiere bienes intracomunitarios libres de IVA y los vende aplicando el impuesto al comprador, sin embargo, dicha sociedad desaparece sin ingresarlo en Hacienda, generando pérdidas millonarias. Todo ello se suele realizar a través de un esquema complejo de empresas y testaferros coordinados para evadir el impuesto y posicionar el producto en el mercado sin competencia al reducir costes.

[47] En este sentido, ya hace diez años se estimó que el fraude MTIC generaba pérdidas del orden de 29,3 mil millones de euros/año en la UE, subrayando su carácter sistémico y su capacidad para explotar asimetrías regulatorias y operativas entre Estados miembros (Savona y Riccardi, 2015).

En España, la ENCODG 2019-2023 determinaba que el fraude asociado al IVA suponía hasta un 18 % de la recaudación prevista, un dato sensiblemente diferente al que se ha expuesto anteriormente del 4,6 % estimado por UE. El contraste ilustra la diferencia entre estimaciones estratégicas y mediciones estadísticas armonizadas más recientes, pero coincide en el diagnóstico: el fraude del IVA supone un menoscabo sustancial y sostenido de ingresos públicos.

España participa activamente en EMPACT en el ámbito MTIC y ha reforzado su cooperación con EPPO/OLAF/EUROPOL, según el informe IASN 2023[48].

3.1.3 Cibercriminalidad económica

El SEPBLAC señala que una de las consecuencias del desarrollo de la digitalización en las relaciones financieras, propiciada por la pandemia del COVID-19, ha sido un notabilísimo aumento del ciberfraude, generando una industrialización de esta actividad ilícita.

Por otro lado, esta entidad subraya el interés de las organizaciones criminales en operar con criptoactivos por favorecer el anonimato (SEPBLAC, 2024).

Pero no solo la cibercriminalidad económica se constriñe al ciberfraude, pues otra operativa sumamente dañina es la denominada como *ransomware*. Además, la modalidad *crime as a service* es una constante en este ámbito delincuencial.

Uno de los medios más eficaces seguidos por esta cibercriminalidad para alcanzar sus objetivos (*ransomware*, fraudes *online* y blanqueo) es la utilización de plataformas de servicios digitales legítimos (redes sociales, *apps*, *marketplaces*, pagos, nube). Estas se configuran como una de las principales «superficies de ataque» que la ciberdelincuencia económica explota y están en el centro de la respuesta estratégica UE-España. A escala UE, millones de ciudadanos son objetivo cada año y se sustraen miles de millones de euros[49].

[48] En este marco, ha introducido medidas regulatorias como el Real Decreto 1007/2023 (requisitos de software de facturación y trazabilidad/verificabilidad para combatir el *sales suppression*), o el establecimiento del uso del Registro de Operadores Intracomunitarios (ROI) y el impulso a equipos conjuntos de investigación en fraudes intracomunitarios.

[49] IOCTA 2024–2025, ENCODG 2025 y Estrategia Nacional de Ciberseguridad.

Por otro lado, la UE[50] y España (ESN 2021, Estrategia Nacional de Ciberseguridad 2019 y Ley 36/2015, de Seguridad Nacional) asumen la ciberseguridad como infraestructura de la seguridad económica.

La inteligencia y la colaboración público-privada es esencial en este ámbito, extremo potenciado por todas las estrategias europeas, nacionales y sectoriales.

3.1.4 Economía derivada del tráfico de drogas

La Estrategia de la UE en materia de lucha contra las drogas 2021-2025, aprobada por el Consejo el 18 de diciembre de 2020, marca como primera prioridad para luchar contra el narcotráfico la asfixia económica de las organizaciones criminales, no permitiendo que los beneficios ilícitos puedan ser introducidos en el sistema legal[51].

Los estudios que EUROPOL ha realizado sobre el tráfico de droga en la UE remarcan el impacto severo que provoca al sistema económico europeo, estimando que el mercado de drogas en la UE asciende a un valor mínimo de al menos 31 000 millones de euros al año, constituyendo una de las fuentes principales de ingresos para la delincuencia organizada (EMCDDA y EUROPOL, 2024).

La ENCO 2025 señala al narcotráfico como el mercado ilícito con mayor capacidad de generación de beneficios ilícitos en España. Detallando que los beneficios derivados del tráfico de drogas se canalizan hacia sectores como la hostelería, inmobiliario, transporte y ocio nocturno, afectando a la competencia y facilitando el blanqueo.

Estudios referidos por el Grupo de Acción Financiera Internacional (GAFI/FATF) indican que las redes dedicadas al narcotráfico suelen utilizar criptoactivos como medio de pago y capa de anonimato, así como empresas pantalla para enmascarar los flujos ilícitos y ocultar su origen (FATF, 2022) y testaferros (Savona y Riccardi, 2015).

---

[50] Communication from the Commission to the European Parliament and the Council: Advancing European economic security: an introduction to five new initiatives. Disponible en: https://commission.europa.eu/system/files/2024-01/Communication%20on%20European%20economic%20security.pdf?utm_ [Consulta: 28 agosto 2025].

[51] Consejo de la UE. Estrategia de la UE sobre drogas 2021-2025. Disponible en: https://www.consilium.europa.eu/media/54074/qc0521073esn_002.pdf [Consulta: 26 agosto 2025].

3.1.5 Delitos contra el mercado y la propiedad intelectual/industrial

Desde una perspectiva global, el comercio de falsificaciones constituye un fenómeno estructural con graves repercusiones económicas y de seguridad. Según el informe conjunto de la Organización para la Cooperación y el Desarrollo (OCDE/OECD) y la EUIPO (2021), el valor del comercio mundial de productos falsificados se estimó en 467 000 millones de dólares, lo que equivale aproximadamente al 2,3 % del comercio mundial. En el caso específico de la UE, las importaciones de falsificaciones ascendieron a 99 000 millones de euros en 2021, representando el 4,7 % del total de importaciones procedentes de terceros países (OECD/EUIPO, 2025).

En España, y únicamente en los sectores de juguetes, cosmética y textil, las pérdidas ascienden a 1511 millones de euros anuales y suponen la destrucción de más de quince mil empleos cada año[52].

Respecto a las actividades fraudulentas de afectación a los mercados, la EU mantiene una regulación básica[53], que establece los términos de manipulación de mercado y los de información privilegiada (incluidas sanciones penales mínimas armonizadas), en virtud del riesgo que suponen para la integridad de los mercados y la confianza pública.

En España, existen dos organismos reguladores para estas cuestiones la CNMV y la CNMC. En 2018, la CNMC creó, en el ámbito de su Dirección de Competencia, la Unidad de Inteligencia Económica (UIE), a la que se ha ido dotando paulatinamente de personal especializado y recursos específicos. Su cometido es la detección de oficio de conductas anticompetitivas, con especial atención a la lucha contra los cárteles (CNMC, 2023).

3.1.6 Criminalidad medioambiental

En el ámbito medioambiental, la ENCO 2025 señala que los delitos asociados a la gestión y tráfico ilegal de residuos, el comer-

[52] Oficina española de patentes y marcas (OEPM). Boletín 162. EUIPO Observatory new study. Enero 2024. Disponible en: https://www.oepm.es/cs/OEPMSite/contenidos/Revista_InfoPYM/2024/Enero/en/noticia3.html?utm_ [Consulta: 29 agosto 2025].

[53] El Reglamento (UE) N.º 596/2014 del Parlamento Europeo y del Consejo, de 16 de abril de 2014, sobre el abuso de mercado (Reglamento sobre abuso de mercado) y la Directiva 2014/57/UE del Parlamento Europeo y del Consejo, de 16 de abril de 2014, sobre las sanciones penales aplicables al abuso de mercado (Directiva sobre abuso de mercado).

cio ilícito de especies protegidas y la explotación irregular de recursos naturales constituyen un desafío creciente para España. Estas prácticas, con frecuencia vinculadas al crimen organizado, no solo provocan graves daños a los ecosistemas, sino que también afectan a la economía formal. Frente a ello, se subraya la importancia de potenciar las redes de inteligencia medioambiental y la cooperación interinstitucional, con el fin de mitigar los impactos más nocivos de esta modalidad criminal[54].

EUROPOL, en su European Financial and Economic Crime Threat Assessment (2023), añade un relativamente nuevo vector en este ámbito, la transición verde, que crea nuevos nichos para el fraude vinculados a la contratación pública mediante la corrupción, extremo que puede lastrar inversiones y objetivos de sostenibilidad si no se acompaña de adecuados controles de integridad.

3.1.7 Trata de seres humanos

La lucha contra la trata de seres humanos es una prioridad para la UE[55]. Es una de las prácticas delictivas más rentables para las organizaciones criminales, con unos costes sociales y económicos muy significativos para la UE. La Estrategia de la Comisión Europea 2021-2025 contra la trata cifra en 2700 millones de euros al año el coste económico de la trata en la UE.

El Plan Estratégico Nacional contra la Trata y la Explotación de Seres Humanos 2021-2023 (PENTRA)[56] ya establecía, en concordancia con la ENCODG 2019 y posteriormente con la ENCODG 2025, la necesidad de intensificar las investigaciones financieras para neutralizar la capacidad económica de las redes criminales

[54] Las estimaciones conjuntas de la OCDE, la UNODC, el PNUMA y la INTERPOL sitúan el valor monetario de toda la criminalidad medioambiental transnacional organizada entre 70 000 y 213 000 millones de dólares estadounidenses anuales (UNICRI, 2016).

[55] Council conclusions on the creation and implementation of a EU policy cycle for organised and serious international crime, 3043rd JUSTICE and HOME AFFAIRS, Council meeting Bruselas, 8 y 9 de noviembre de 2010. Disponible en: https://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/en/jha/117583.pdf [Consulta: 28 agosto 2025].

[56] El plan se evaluó en 2024, con la intención de elaborar una nueva estrategia para erradicar esta actividad delictiva. https://www.interior.gob.es/opencms/es/detalle/articulo/Las-Fuerzas-y-Cuerpos-de-Seguridad-del-Estado-liberaron-a-1.466-victimas-de-trata-y-explotacion-en-2023-un-24-por-ciento-mas-que-en-2022/#:~:text=BALANCE%20DEL%20PLAN%20ESTRAT%C3%89GICO%20NACIONAL,trata%20y%20explotaci%C3%B3n%20de%20personas [Consulta: 28 agosto 2025].

dedica a esta actividad delictiva, así como generar inteligencia que pueda ser empleada en la lucha contra esta lacra social[57].

3.1.8 Corrupción

La corrupción constituye un fenómeno transversal que afecta a la totalidad de los ámbitos delictivos analizados y que se erige como un facilitador crítico (junto con el blanqueo de capitales y el uso de estructuras empresariales legales) de la delincuencia organizada y grave. Su capacidad para erosionar la integridad institucional, distorsionar la competencia económica y debilitar la confianza en el Estado de Derecho (Blackburn *et al*., 2017) la convierte en una amenaza prioritaria tanto para la UE como para España.

A escala europea, el SOCTA 2025 de EUROPOL identifica la corrupción como un instrumento recurrente de las redes criminales, empleado para infiltrarse en la economía legal, manipular contrataciones públicas, asegurar impunidad y neutralizar controles regulatorios.

En España, la ENCODG 2025, en concordancia otra vez con la estrategia europea, considera a la corrupción como un fenómeno trasversal en la criminalidad organizada y grave[58], con incidencias múltiples en la seguridad nacional, debilitando los pilares del buen Gobierno, generando desconfianza y deterioro institucional, infiltrándose en infraestructuras y obstruyendo la acción de la justicia.

En este marco, cabe señalar que el Gobierno español aprobó, el 26 de agosto del 2025, el Plan de Lucha contra la Corrupción[59] y creó una Comisión Interministerial para su puesta en marcha y seguimiento[60], recogiendo las recomendaciones del Grupo de

[57] CITCO. PENTRA. Disponible en: https://www.interior.gob.es/opencms/pdf/prensa/balances-e-informes/2021/220112_Plan_nacional_TSH_PENTRA_FINAL_2021_2023.pdf [Consulta: 28 agosto 2025].

[58] Entre sus líneas de acción, prevé potenciar la detección y neutralización de los delitos de corrupción, mejorar procedimientos en áreas vulnerables a la infiltración criminal y reforzar las investigaciones financieras y la recuperación de activos.

[59] Vicepresidencia Primera del Gobierno. Ministerio de Hacienda. Nota de prensa. Disponible en: https://www.hacienda.gob.es/es-ES/Prensa/Noticias/Paginas/2025/20250826-NP-CM-LUCHA-CONTRA-CORRUPCION.aspx [Consulta: 28 agosto 2025].

[60] Real Decreto 711/2025, de 26 de agosto, por el que sea crea la Comisión Interministerial para el impulso del Plan Estatal de Lucha contra la Corrupción, y se establece

Estados contra la Corrupción del Consejo de Europa (GRECO)[61], de la OCDE, la Comisión Europea y de la sociedad civil. Destacando la potenciación del *Big Data* y la AI en el marco de la contratación pública, así como una especial atención al fraude asociado a fondos europeos.

3.2 Sectores con mayor penetración criminal, perspectiva económica

Como se ha expuesto, la evidencia europea y española muestra que la delincuencia organizada y grave penetra preferentemente en sectores intensivos en efectivo, con barreras de entrada bajas o donde puede utilizar estructuras legales (sociedades, fundaciones, testaferros, contratos, licitaciones públicas, etc.) para dar cobertura y legitimidad a actividades ilícitas, así como blanquear los bienes ilícitos.

Además, se debe apuntar que España resulta mucho más atractiva que otros países de su entorno para la DO y la DG por distintos factores geográficos, logísticos, estructurales y económicos (Balas Dávila, 2023).

En virtud de todo lo anterior, los sectores que soportan el mayor impacto de injerencia de esta criminalidad organizada y grave son:

- Sector energético e infraestructuras críticas

El sector energético, en su doble dimensión de actividad económica esencial y de infraestructura crítica, constituye un ámbito de particular vulnerabilidad frente a la delincuencia organizada y grave.

El caso del fraude en los hidrocarburos es paradigmático, según el SOCTA 2025, se lleva a cabo a través de estructuras criminales complejas que gestionan toda la cadena de suministro y la distribución minorista[62].

---

su composición y funcionamiento. Disponible en: https://www.boe.es/diario_boe/txt.php?id=BOE-A-2025-17185 [Consulta: 28 agosto 2025].

61 El Grupo de Estados contra la Corrupción (GRECO) es un órgano del Consejo de Europa creado en 1999 para supervisar las políticas anticorrupción y ayudar a sus Estados miembros a mejorar su capacidad de prevención y lucha contra la corrupción a través de la evaluación de sus sistemas. El GRECO incluye a los 46 miembros del Consejo de Europa, Estados Unidos y Kazajistán.

62 De este modo, los delincuentes implicados en el fraude de combustibles dependen de la experiencia de profesionales, como químicos y trabajadores del sector petrolero.

– Servicios financieros, pagos y criptoactivos

Este sector es uno de los de mayor riesgo por estar expuesto, constantemente, a dinámicas de blanqueo de capitales llevadas a cabo por la generalidad de la delincuencia grave y organizada.

Por ello, su monitorización es exhaustiva y constante por las diferentes unidades de inteligencia financiera de los distintos países, siendo esta función desarrollada por el SEPBLAC en España.

– Construcción e inmobiliario

La inversión en inmuebles y construcción es una de las vías más frecuentes para colocar y estratificar fondos ilícitos, al constituir un sector intensivo en capital, con una elevada capacidad de enmascaramiento y valorización, donde el uso criminal de profesionales (abogados, agentes, notarios) y estructuras societarias está muy expandido (Europol, 2023).

– Hostelería, restauración, ocio y turismo

Bares, restaurantes, hoteles y locales de ocio, en general, son también negocios intensivos en efectivo idóneos para mezclar flujos ilícitos con ventas legítimas y para encajar empleo irregular (Savona y Riccardi, 2015). Es decir, constituyen otro instrumento para blanquear los bienes ilícitos obtenidos.

– Comercio mayorista/minorista, *e-commerce* y fraude de impuestos

El comercio, en general, se ve afectado por la competencia desleal que llevan a cabo la delincuencia organizada y grave a través de la ventaja competitiva que le proporciona la falsificación, la denominada piratería, y por la omisión en la satisfacción de las cargas fiscales[63].

En este ámbito también se incluye las distintas formas de contrabando, siendo un valor refugio para las organizaciones criminales, el contrabando y la falsificación de tabaco.

– Transporte, logística y puertos

El fraude documental, como la declaración falsa de mercancías transportadas, está plenamente implantado en estas prácticas fraudulentas.

[63] Los sectores donde sufren con insistencia este desgaste son: industria cultural y creativa (música, cine, software, videojuegos, literatura), moda y textil, industria farmacéutica y cosmética, automoción y repuestos, agroalimentario y pesticidas, así como componentes tecnológicos.

Las organizaciones criminales emplean empresas de transporte y logística (incluidos agentes transitarios, depósitos fiscales y almacenes) para mover mercancías ilícitas y legitimar flujos comerciales. Estas acciones, frecuentemente, se encuentran vinculadas con prácticas corruptoras, llegando a constituirse nodos de corrupción.

– Gestión de residuos, reciclaje y medio ambiente

La gestión de residuos, energías renovables y actividades conexas presentan barreras regulatorias aprovechables y márgenes elevados. En este contexto, la concurrencia de manipulación de licencias y vertidos y el abuso de la subcontratación proyecta efectos de dumping ambiental[64] y de competencia desleal (EUROPOL, 2023; UNICRI, 2016).

– Contratación pública

La contratación pública constituye uno de los sectores más vulnerables a la penetración de la delincuencia organizada y la corrupción, debido al elevado volumen de recursos que gestiona y a la posibilidad de influir en la asignación de contratos y licitaciones. Tanto EUROPOL como EUROJUST han señalado que este ámbito es un objetivo prioritario de las redes criminales y corruptas, ya que facilita la creación de estructuras cuasimonopólicas mediante prácticas como la manipulación de concursos, el soborno o la colusión entre empresas y funcionarios, distorsionando la competencia y erosionando la confianza institucional.

4 Las investigaciones económicas

Tanto las estrategias nacionales españolas como las europeas destacan que investigar la dimensión económica de la amenaza que supone la delincuencia organizada y grave es crucial para neutralizarla. Por ello, el desarrollo de investigaciones de naturaleza económica se ha convertido en un pilar esencial para salvaguardar la integridad del sistema financiero (que pone en riesgo la DO y la DG) y, por ende, la seguridad nacional.

Las investigaciones económicas aglutinan las tres tipologías básicas que concurren en la indagatoria criminal: investigación de actividad, investigación de hechos e investigación documental.

[64] Práctica competitiva por la que una empresa o un país obtiene ventaja de costes al producir o vender aprovechando exigencias ambientales más laxas.

Esta concurrencia es requerida por la complejidad de perfeccionar los tipos penales asociados a los diferentes delitos de índole económico. Sirva de referencia de esta dificultad el hecho de que el blanqueo de capitales se configura como una de las tipologías delictivas que habitualmente se corrobora por prueba indiciaria[65].

La redundancia de indicios, a través de las tres tipologías expuestas, facilita la comprensión de la correspondencia de los hechos con los elementos del tipo.

En este marco de complejidad, es perentorio la IE, mediante la cual se facilita el enfoque inicial de la investigación, pudiendo también reforzarla de manera directa con la aportación de información muy especializada y que, en determinados casos, únicamente puede ser aportada por los propios sectores afectados, debido a su especificidad.

En este sentido, la estructura de una investigación económica suele involucrar múltiples fases y actores, combinando las técnicas clásicas de investigación criminal con herramientas propias del análisis financiero. En términos generales, un caso típico se desarrolla en cuatro fases fundamentales: policial, preprocesal, judicial y posexplotación.

La aportación de IE en cada una de estas fases aporta calidad a la investigación y contribuye a su eficacia (EUROPOL, 2017) (FATF, 2012).

4.1 Estructura de una investigación económica

– Fase policial

Es aquella que desarrolla la unidad policial investigadora de manera autónoma y suele ser el inicio de la investigación criminal.

El origen de esta actividad se vincula, en muchas ocasiones, a la recepción de IE, la cual puede provenir de actores que tienen normalizada la elaboración de inteligencia y su difusión como OLAF, AEAT o SEPBLAC, o por otros actores como asociaciones sectoriales que ven afectados sus intereses [por ejemplo, Sociedad

[65] En concordancia con lo dictado por la STS 801/2010, de 23 de septiembre de 2010 y, también, la STS 645/2023, 25 de julio de 2023. En concomitancia con ello, la «comunicación por indicio» es obligatoria para sujetos obligados (Ley 10/2010 de 28 de abril, de prevención del blanqueo de capitales y de la financiación del terrorismo), información esencial para elaborar los informes de inteligencia elaborados por el SEPBLAC. Esto no es «prueba indiciaria» penal, pero explica por qué, en la práctica, los casos de blanqueo llegan a sede penal con indicios concatenados

General de Autores y Editores (SGAE)] que generan informes *ad hoc* sobre alguna supuesta práctica fraudulenta del sector, o por diferente información de trabajadores y directivos de empresas que observan malas praxis que la entidad encubre de manera deliberada, etc.

En esta etapa, la información es fragmentaria y debe valorarse su fiabilidad y relevancia. Si se aprecia verosimilitud, se define un plan de obtención y se activa la correspondiente coordinación interagencial. De igual modo, cuando se detecta una proyección internacional, se conforma, ya en estos estadios iniciales, el apoyo de organismos internacionales como EUROPOL/EFECC u OLAF.

De esta forma, la IE recibida se intenta corroborar a través de diferentes comprobaciones de distinta naturaleza, para a continuación conectarla con hechos y entidades concretas compatibles con una tipología delictiva.

– Fase preprocesal

Esta se desarrolla en el marco de las diligencias de investigación desarrolladas por el Ministerio Fiscal[66] o por el procedimiento de investigación que incoe la EPPO[67]. Identificado el posible delito económico se consolida la estrategia.

En este sentido, se integran, bajo la tutela de las diferentes fiscalías, los primeros grupos interdisciplinares de investigación, este extremo se facilita cuando existen unidades de apoyo o adscritas a las distintas fiscalías.

Igualmente, se requiere, a través de las distintas fiscalías, la remisión de más inteligencia e información económica concreta, fundamentalmente, financiera, fiscal, aduanera, auditoría pública y de sectores afectados, a los actores que de manera normalizada generan dicha inteligencia[68].

[66] Artículo 773 de la LECrim, artículo 5 de la Ley 50/1981, de 30 de diciembre, por la que se regula el Estatuto Orgánico del Ministerio Fiscal y Circular 4/2013 de la Fiscalía General del Estado (FGE).

[67] Artículo 17 de la Ley Orgánica 9/2021, de 1 de julio, de aplicación del Reglamento (UE) 2017/1939 del Consejo, de 12 de octubre de 2017, por el que se establece una cooperación reforzada para la creación de la Fiscalía Europea.

[68] Según la Memoria 2022-2023 del SEPBLAC, este organismo remitió 97 informes de inteligencia financiera. Del mismo modo, el Informe OLAF 2024 detallaba que 74 casos fueron remitidos por OLAF a la EPPO. Mientras que el Tribunal de Cuentas remitió un caso a Fiscalía apreciando responsabilidad penal, según la Memoria 2024 de la Fiscalía General del Estado.

Debido a la dilatación de las respuestas de los distintos organismos a los requerimientos de índole económico, esta fase es muy utilizada por dos cuestiones, la primera, porque alarga el tiempo de la indagatoria sin estar constreñida a lo marcado en las causas judicializadas, y la segunda, porque posibilita una base fáctica y documental más sólida[69], para la apertura de las diligencias judiciales pertinentes.

Si las distintas fiscalías entienden que concurren en los hechos investigados algún ilícito penal, procederá a conformar una denuncia ante la autoridad judicial solicitando la instrucción de las oportunas diligencias judiciales.

– Fase judicial

Esta es la fase nuclear de cualquier investigación criminal y la dirección corresponde a la autoridad judicial competente. Aquí se desarrollan, de manera mucho más concreta, las líneas de investigación que mantengan una mayor carga probatoria. En este sentido, se seguirá recabando información e inteligencia de las distintas fuentes[70], normalizadas o no normalizadas mediante las diligencias necesarias que estime el órgano instructor[71].

Es en esta fase donde, se pueden acordar medidas de investigación limitativas de derechos fundamentales, como la interceptación de comunicaciones telefónicas y telemáticas y la captación y grabación de comunicaciones orales mediante dispositivos electrónicos, así como el uso de dispositivos técnicos de seguimiento y localización[72], al objeto de convertir la inteligencia financiera que se obtenga de estas actuaciones en impacto operativo (EUROPOL, 2017).

Una vez se tienen indicios suficientes sobre las entidades que participan en los supuestos hechos delictivos investigados, la autoridad judicial determinará la práctica de nuevas diligencias con el fin de alcanzar determinada información que de otro modo no sería posible obtener, alguna de ellas pueden consistir en entradas y registros o detenciones. La práctica del conjunto de

[69] Circular 4/2013 de la FGE, sobre las diligencias de investigación.

[70] La Memoria de actividades de la IGAE 2024 identifica actuaciones en 87 procedimientos bajo la fórmula de auxilio judicial. El Informe anual de la CNMV 2024 muestra que se actuó en sesenta ocasiones en el ámbito penal por requerimientos de la autoridad judicial o Fiscalía. La Memoria de la CNMC 2023 refleja 1051 actuaciones ante solicitudes de Juzgados y Tribunales, así como otras administraciones públicas.

[71] Artículo 774.1 de la LECrim.

[72] Artículos 588 ter, 588 quater y 588 quinquies de la LECrim.

estas diligencias se denomina, en el desarrollo de la investigación criminal policial, explotación de la investigación.

– Fase posexplotación

  Realmente, esta etapa sigue bajo la tutela de la instrucción judicial, pero se diferencia de la anterior porque la perspectiva investigativa cambia. Aunque sigue bajo la dirección del órgano judicial de la instrucción, en esta fase el énfasis de la investigación transita desde la obtención de evidencias a su tratamiento y análisis intensivo.

  El corpus documental que llega a esta fase suele ser voluminoso y no normalizado: entradas y registros, interceptaciones de comunicaciones, seguimientos/localizaciones, y, muy especialmente, registros y volcados forenses de dispositivos electrónicos y acceso remoto a sistemas, todo ello obtenido bajo autorización judicial.

  Dado el volumen y heterogeneidad de la información (documental, financiera, digital), esta etapa es eminentemente analítica, en la cual se depuran, correlacionan y visualizan los patrones y los flujos, para determinar la trazabilidad y posibles conversiones de los bienes ilícitamente obtenidos, priorizando objetivos y articulando medidas de recuperación de activos.

En este sentido, los organismos internacionales recomiendan el uso de analítica avanzada como *Big Data* y aprendizaje automático para generar inteligencia financiera que pueda ser utilizada de manera efectiva en el procedimiento judicial.

Tras el análisis de todo lo intervenido en la explotación, la Policía Judicial y los peritos elevan informes complementarios al Juzgado. Tras lo cual, y siguiendo los trámites oportunos, el instructor judicial remite la causa al órgano de enjuiciamiento, con lo que culmina la fase instructora y se inicia la de juicio oral.

En suma, las investigaciones económicas, en sentido amplio, abarcan todas aquellas pesquisas orientadas a desentrañar las estructuras financieras, patrimoniales y comerciales detrás de actividades ilícitas complejas.

Su finalidad va más allá de la mera persecución penal individual, buscando neutralizar las redes criminales atacando su capacidad económica, privándolas de ganancias ilícitas y desarticulando sus entramados empresariales.

Así, el enfoque económico complementa las investigaciones tradicionales, añadiendo una capa de análisis que permite identificar a los beneficiarios finales, detectar vínculos ocultos entre delincuentes y aparentes negocios legales, y descubrir flujos financieros opacos que alimentan actividades delictivas. Todo ello requiere de metodologías rigurosas, personal especializado (analistas financieros, peritos contables, etc.) y, sobre todo, de una adecuada integración de la IE en el proceso investigador.

4.2 Integración de la inteligencia económica en las investigaciones

Para que un proceso de inteligencia sea operativo y útil en investigación, no puede desarrollarse de forma aislada, es decir, debe conectarse estrechamente con la investigación judicial y fiscal, a través de los organismos policiales competentes encargados de materializar las pesquisas.

En otras palabras, la inteligencia (como conocimiento analítico) solo adquiere pleno valor cuando fluye hacia la acción investigadora, guiando a quienes tienen la potestad legal de obtener pruebas y perseguir delitos. Este principio de integración ha sido destacado tanto por expertos como por las propias instituciones.

En términos sustantivos, la coordinación y cooperación tempranas entre analistas de inteligencia e investigadores permite orientar desde el inicio las líneas de indagación hacia indicios de difícil detección (como cuentas en jurisdicciones de baja tributación y alta opacidad o la utilización de testaferros internacionales) antes de que se disipen o desaparezcan, lo que incrementa de forma significativa la eficacia de la investigación.

En España, la integración de la IE en las investigaciones se enfrenta al desafío de la ausencia de un SIE formal, pero cuenta con mecanismos parciales de coordinación que se han ido desarrollando en distintos ámbitos.

Uno de ellos es el Departamento de Seguridad Nacional (DSN), órgano de la Presidencia del Gobierno que integra análisis interministeriales sobre riesgos estratégicos, incluyendo los económicos.

No obstante, los intercambios en el máximo nivel estratégico no se traducen automáticamente en mecanismos operativos estables. Diversos análisis recomiendan institucionalizar dichos intercambios (objetivo que perseguía el no implementado SIE) para

que la cooperación no dependa de la mera buena voluntad personal ni de iniciativas *ad hoc*.

En consecuencia, se aprecia la necesidad de reforzar los órganos nacionales de coordinación en inteligencia económica y dotarlos de procedimientos normalizados de trabajo, canales permanentes de intercambio de información y circuitos de retroalimentación que conecten de forma estructurada y continua la inteligencia estratégica (orientada a riesgos económicos sistémicos) con las unidades investigadoras de investigación criminal.

Un caso práctico de unidad de fusión operativa es el mencionado CITCO, adscrito al Ministerio del Interior. Con rango de subdirección general, el CITCO recibe, integra y analiza la información estratégica que le proporcionan todas las fuerzas y cuerpos de seguridad sobre delincuencia organizada, criminalidad grave, terrorismo y radicalización, elaborando inteligencia criminal de carácter estratégico, prospectivo, pero también operativo.

En este sentido, actúa como punto de contacto nacional para el intercambio de inteligencia con organismos internacionales, manteniendo relaciones con centros homólogos de la UE (EUROPOL) y de terceros países. En la práctica, el CITCO coordina la elaboración de valoraciones nacionales de amenaza y la respuesta unificada a fenómenos que trascienden el ámbito de una sola agencia.

Su rol ilustra cómo integrar inteligencia en investigaciones: por un lado, gestiona información de múltiples fuentes policiales (y de otras agencias) para producir análisis integrados. Por otro, retroalimenta a las unidades investigadoras con dichas valoraciones, señalando prioridades, conexiones entre casos y tendencias emergentes.

En suma, el CITCO funciona como un modelo sectorial de integración: es un *hub* donde converge la inteligencia criminal y desde el que se articula la cooperación tanto interinstitucional (entre cuerpos de seguridad y ministerios) como internacional.

La Estrategia Nacional contra el Crimen Organizado 2019-2023 apunta que debe potenciarse el papel del CITCO para mejorar la coordinación efectiva de investigaciones[73].

[73] También recalca la importancia de que CITCO elabore inteligencia estratégica útil y facilite investigaciones conjuntas cuando las tramas criminales operan en múltiples ámbitos delictivos.

El enfoque colaborativo público-privado es esencial, pues muchas informaciones críticas residen en empresas (entidades bancarias, compañías energéticas, telecomunicaciones o grandes corporaciones tecnológicas) que deben cooperar estrechamente con el Estado para detectar distintos riesgos económicos.

Algunos pasos ya se han dado en esa dirección bajo el paraguas del CNPIC, existiendo convenios con empresas estratégicas para intercambiar información de inteligencia sobre amenazas, muchas de ellas económicas.

En el plano operativo, la integración de la inteligencia económica implica también mejorar el tránsito de la información entre agencias con competencias distintas. Un punto crítico es asegurar que la inteligencia financiera (procedente de UIF, AEAT, órganos supervisores, entidades reguladoras, etc.) pueda ser compartida en tiempo y forma con las unidades investigadoras policiales y judiciales, superando barreras legales o burocráticas en los momentos iniciales de una investigación.

A este respecto, la Ley Orgánica 9/2022, de 28 de julio, por la que se establecen normas que facilitan el uso de información financiera y de otro tipo para la prevención, detección, investigación o enjuiciamiento de infracciones penales en España, que transpone directivas europeas, establece cauces suficientemente ágiles para que la inteligencia accionable gestionada por el SEPBLAC pueda ser distribuida oportunamente a las fuerzas de seguridad y al Ministerio Fiscal.

A nivel europeo, la integración de la IE en las investigaciones es ya una realidad institucionalizada en varios frentes. EUROPOL cuenta con centros especializados, como el mencionado EFECC, dedicados a apoyar a los Estados miembros en casos de delincuencia financiera compleja.

EUROPOL recopila y analiza datos de inteligencia aportados por las diferentes policías nacionales siguiendo protocolos estandarizados, enriqueciendo esta información con fuentes complementarias (informes de *open sources*, investigación académica y casos de estudio). El resultado son productos de inteligencia que transfiere a los distintos cuerpos policiales de los diferentes países, posibilitando, también, la articulación de equipos conjuntos.

Tales análisis conjuntos trabajan en la prevención, permitiendo a las fuerzas de seguridad anticiparse a las tendencias delictivas y orientar mejor sus recursos.

Como ya se ha detallado, existen otros organismos como OLAF y la EPPO, que también juegan un papel integrador. OLAF investiga el fraude que afecta al presupuesto de la UE, generando inteligencia que luego se transfiere a EPPO para su judicialización cuando procede, así como a los países miembros.

En síntesis, la integración de la IE en las investigaciones es un requisito indispensable para afrontar con éxito las amenazas actuales. La UE ha ido institucionalizando un enfoque integrado, situando la inteligencia financiera en el centro de la identificación, anticipación y neutralización de las formas más lesivas de criminalidad organizada.

Para España, avanzar en esta misma línea supone reforzar los mecanismos de coordinación (DSN, CITCO, comités especializados, etc.) y asegurar que todos los procesos de IE tengan un cauce directo hacia la investigación criminal a través de las fuerzas y cuerpos de seguridad competentes y el Ministerio Fiscal.

Dados los hallazgos expuestos (inexistencia de un SIE formalmente definido, mecanismos solo parciales de coordinación y necesidad de cauces estables entre la inteligencia estratégica y las unidades investigadoras), resulta pertinente, en este punto, valorar la creación de un órgano colector con capacidad para absorber la inteligencia de interés para la seguridad nacional, filtrándola y clasificándola conforme al listado de riesgos y amenazas de la ESN, que incluye la DO y la DG.

En el ámbito de la DO y la DG, la inteligencia criminal, incluida la IE procedente de distintos generadores, debería compartirse sistemáticamente con el CITCO, como nodo de fusión y coordinación operativa entre las FCS, con proyección internacional. A efectos de diseño institucional, el DSN se perfila como candidato idóneo para ejercer ese rol de colector que aglutine, gestione y transfiera al CITCO la inteligencia, por su vinculación con el Consejo de Seguridad Nacional y su ubicación en el Gabinete de la Presidencia (Dirección Adjunta), donde se integra la Oficina de Asuntos Económicos y G-20.

No obstante, su puesta en marcha exigiría, en su caso, adecuaciones normativas y dotaciones específicas (procedimientos normalizados, capacidades técnicas y humanas, así como circuitos de retroalimentación con las unidades investigadoras).

Solo así la inteligencia dejará de ser un mero producto teórico para convertirse en palanca efectiva que impulse investigaciones,

desarticule tramas criminales y contribuya a la preservación de la seguridad económica y con ello a la seguridad nacional.

4.3 Necesidades de información no normalizada en las investigaciones económicas

Una de las lecciones derivadas de la experiencia en investigaciones financieras complejas es que, con frecuencia, la información convencional no basta. Las organizaciones criminales aprenden a explotar vacíos y a mimetizarse con la economía legal, de modo que muchas de sus actividades ilícitas no quedan registradas de forma directa, de manera evidente, en ningún registro oficial.

Por ello, las investigaciones económicas requieren acceder a información no normalizada, es decir, a fuentes y a tipos de datos que no siguen los esquemas tradicionales o que no están integrados en los canales formales de intercambio entre agencias. Este tipo de información puede incluir desde documentación informal hasta inteligencia prospectiva o fuentes abiertas, y suele ser imprescindible para llenar los vacíos de conocimiento sobre una trama delictiva.

Por información no normalizada se puede entender, en primer lugar, aquella que no está estandarizada ni estructurada en registros oficiales. Un ejemplo típico son los datos procedentes de fuentes abiertas (OSINT): noticias de prensa, publicaciones en redes sociales, *blogs* financieros, foros de Internet e incluso filtraciones como los denominados periodísticamente «papeles de Panamá". Este tipo de información, aunque inicialmente no verificada, puede aportar indicios valiosos.

La inteligencia de fuentes abiertas se ha convertido en una disciplina en sí misma dentro del análisis económico: proporciona contexto sobre tendencias de mercado, perfiles reputacionales de individuos y empresas, conexiones globales, etc., que, difícilmente, se obtienen de bases de datos estructuradas.

Integrar OSINT en las investigaciones económicas implica dotarse de herramientas para cribar grandes volúmenes de información en Internet, usar algoritmos de búsqueda avanzada y contar con analistas capaces de separar rumor del dato comprobable.

Otro ámbito de información no normalizada son los datos comerciales y registros extranjeros. Seguir la pista a estas empresas requiere obtener información societaria de múltiples jurisdiccio-

nes, la cual no está unificada ni viene en formatos homogéneos, y donde la cooperación judicial internacional es esencial.

Todo esto constituye información «no normalizada» en tanto que no existe una base de datos única ni un estándar global para acceder a ella. Para salvar este escollo, las investigaciones económicas cuentan, cada vez más, con redes de colaboración internacional.

Estas diligencias generan un flujo de información heterogénea, desde extractos bancarios hasta testimonios de testigos, que debe integrarse cuidadosamente en la respectiva investigación nacional.

Asimismo, bajo la categoría de información no normalizada entran las técnicas especiales de obtención de información propias de los servicios de inteligencia o de las investigaciones encubiertas.

Por ejemplo, puede recabarse información a través de colaboradores o informantes en el mundo empresarial (HUMINT), cuyos aportes no siguen un formato predefinido y cuyo valor depende de la evaluación cualitativa que haga el analista.

Del mismo modo, operaciones de vigilancia electrónica (intervenciones de comunicaciones, rastreo de correos electrónicos, etc.) generan un volumen masivo de datos (grabaciones de voz, *logs*, mensajes, etc.) que no están ordenados para su uso inmediato y requieren un procesamiento intensivo para extraer la inteligencia accionable.

Por ejemplo, interceptar miles de correos de una empresa investigada produce un *dataset* no estructurado donde solo técnicas de análisis semántico o búsqueda por palabras clave podrán identificar menciones a pagos ilícitos o códigos que oculten transacciones.

La inteligencia de señales o SIGINT, que incluye escuchas telefónicas, análisis de tráfico de comunicaciones, etc., es otra fuente de datos primarios que puede resultar decisiva para entender la mecánica de ciertos fraudes (por ejemplo, la identificación de responsabilidades y roles dentro de una organización criminal compleja), pero que inicialmente se presenta como información dispersa que ha de ser organizada y correlacionada con la información financiera obrante.

En el contexto de las investigaciones económicas, gestionar información no normalizada implica dotarse de capacidades analíticas y tecnológicas avanzadas. Herramientas de *data mining*, IA

y análisis de redes pueden convertir datos caóticos en patrones inteligibles. De igual forma, técnicas de *machine learning* permiten identificar anomalías en series temporales de transacciones bancarias que no serían evidentes a simple vista.

Estas tecnologías son indispensables para explotar la información no estructurada, pero a su vez requieren analistas capacitados para entrenar los modelos, interpretar los resultados y contextualizarlos correctamente, lo que supone la participación e integración en el equipo investigador de especialistas de diferentes ámbitos, más allá de los analistas económicos.

Finalmente, es importante resaltar que la información no normalizada debe ser tratada con rigor metodológico. Su naturaleza heterogénea puede abrir la puerta a errores si no se somete a un escrutinio adecuado. La calidad de la inteligencia producida dependerá de la capacidad para evaluar la fiabilidad de cada dato y fuente, para verificar la información por vías independientes y para documentar su cadena de custodia cuando vaya a incorporarse a un procedimiento judicial.

En este sentido, las investigaciones económicas exitosas suelen caracterizarse por un escrupuloso trabajo de validación: cada informe externo se contrasta con evidencias propias, cada dato crítico se apoya en al menos una fuente adicional. Así se evitan sesgos cognitivos y se garantiza que la imagen final reconstruida de la actividad económica investigada sea lo más fidedigna posible.

La meta última es que la autoridad judicial competente tenga a su disposición toda la información que necesite para su valoración jurisdiccional, en unas condiciones adecuadas de uso e integridad.

Por ello, la incorporación de información no normalizada, por muy atípica que sea su origen o formato, se erige en indispensable para perfeccionar ese objetivo: proveer a los decisores (jueces, fiscales y altos responsables de seguridad) del conocimiento completo y oportuno para tomar decisiones informadas y efectivas en la lucha contra las amenazas económico-financieras.

5 Conclusiones

Este documento constata la inexistencia en España de un SIE formalmente definido e institucionalizado, de modo que, la función

de IE se dispersa entre múltiples entidades sin una coordinación centralizada, lo que, inevitablemente, genera lagunas, enfoques dispares y dificultades para articular una respuesta unificada, adecuada y oportuna frente a las amenazas económico-financieras de la DO y la DG, respecto a la seguridad nacional.

Esta carencia estructural, provoca la incapacidad de generar una inteligencia integrada y global que aporte el valor añadido derivado de la recolección de información y de las diferentes perspectivas de los distintos actores que conforman el sistema económico descrito. Por lo que se evidencia la imposibilidad de generar una IE adecuada y oportuna, más allá de la actuación en determinados ámbitos vinculados a tipologías delictivas concretas.

Por otro lado, la complejidad competencial y la asimetría entre administraciones (incluso dentro del mismo nivel), así como la cesión de soberanía económica a la UE, dificulta la difusión de IE accionable que pudieran emanar de las entidades integradas en los distintos niveles, no existiendo un dispositivo operativo estable que garantice una integración homogénea de la IE y, menos aún, que permita alcanzar una deseable retroalimentación.

Asimismo, aunque el estudio reconoce mecanismos parciales de coordinación, subraya que los intercambios en el nivel estratégico no se traducen de forma automática en mecanismos estables y operables. Observando, igualmente, que la participación de diferentes órganos generadores de inteligencia, cuando cooperan en la lucha contra la DO y la DG, lo hacen de manera reactiva, sobre cuestiones concretas y ante revelaciones determinadas, es decir, por requerimiento de los responsables de la investigación criminal. Este extremo lastra definitivamente el factor oportunidad.

En el plano operativo-probatorio, se evidencia la necesidad de una formalización metodológica para tratar la información no normalizada. Aunque la normativa reciente facilita el uso de información financiera y su circulación hacia fuerzas de seguridad y Ministerio Fiscal, el estudio muestra que la explotación transversal de la IE presenta gradientes de madurez y barreras legales o burocráticas en momentos iniciales de la investigación, lo que afecta a la oportunidad del empleo de la inteligencia.

En coherencia con este diagnóstico, se propone valorar la habilitación normativa y material de un órgano colector de IE en el DSN, con canalización sistemática hacia el CITCO en materia de DO y DG, como mecanismo para convertir la IE en inteligencia oportuna y accionable en investigación.

Sin embargo, resulta evidente, en relación con todo lo anterior, que la IE financiera se ha institucionalizado como capacidad crítica para detectar, documentar y perseguir la DO y la DG, revelándose que su integración temprana mejora la focalización, la oportunidad y la calidad probatoria a lo largo del caso.

En este marco, la inteligencia tributaria (AEAT/ONIF) y aduanera (ONI/SVA) son palancas operativas con impacto directo en la protección de la seguridad económica (recaudación, competencia leal, integridad de mercados y flujos).

Del mismo modo, la UE ha interiorizado la IE como eje vertebrador de sus políticas de seguridad, institucionalizando un enfoque integrado que sitúa la dimensión financiera y económica en el centro de la identificación, anticipación y neutralización de las amenazas delictivas más graves, y que sirve de fundamento para iniciativas y planes estratégicos conjuntos a escala comunitaria.

En coherencia con ello, España ha avanzado en un alineamiento progresivo con estos marcos, manteniendo sus estrategias y planes nacionales de seguridad económica congruentes con las prioridades europeas e incorporando, entre las amenazas prioritarias, el crimen organizado de carácter financiero.

Existe colaboración efectiva de la CNMC y la Comisión Nacional del Mercado de Valores (CNMV) con autoridades judiciales, esencialmente, a requerimiento de estas. El reto consiste en sistematizar la explotación operativa de su inteligencia sectorial en casos penales complejos y mejorar su interoperabilidad con los canales financieros-fiscales-aduaneros, así como una aportación a las investigaciones criminales de manera proactiva y temprana.

En España existe, al menos conceptualmente, una comunidad de inteligencia ampliada que abarca el ámbito económico y que se integra con la UE. Más allá de los servicios clásicos de inteligencia y seguridad, este estudio constata la participación de un ecosistema más amplio de actores en la generación de inteligencia económica (ministerios económicos, reguladores, sector privado, academia, etc.), en línea con la visión holística promovida a nivel europeo.

En el ámbito de la indagatoria criminal, se propone consolidar equipos conjuntos y circuitos de retroalimentación operativa entre, al menos, SEPBLAC, FCS, AEAT y Ministerio Fiscal desde fases tempranas (policial y preprocesal), articulando cauces similares a los recogidos en la LO 9/2022 y utilizando canales estan-

darizados de intercambio de información como los existentes entre CITCO, EFECC, OLAF y EPPO.

Por tanto, para maximizar la explotación judicial, resulta necesario reforzar recursos humanos especializados (finanzas, datos/IA, cripto y forense digital) y clarificar el uso procesal de la IE mediante metodologías de documentación, verificabilidad y cadena de custodia, apoyadas por una unidad legal con guías y plantillas probatorias, formación a operadores y, en su caso, ajustes normativos acotados.

Con este conjunto coherente de medidas, las propuestas operativizan los hallazgos y permiten transitar de un modelo reactivo a uno anticipatorio, elevando la oportunidad (tiempo de llegada de la IE accionable) y la adecuación (relevancia y utilidad probatoria) en investigaciones económico-penales complejas.

Bibliografía

Arcos, R. (2012). Hacia un Sistema Español de Inteligencia para la seguridad económica y la competitividad [en línea]. Inteligencia y Seguridad. N.º 11, pp. 103-128. [Consulta: 2026]. Disponible en: https://rubenarcos.com/wp-content/uploads/2017/04/11.pdf

Balas Dávila, A. (2023). La financiación de la delincuencia organizada. *Cuadernos de la Guardia Civil*. N.º 69, pp. 49-70.

Buzan, B. (1991). People, States and Fear. An Agenda for International Security Studies in the post-Cold War Era. Hemel Hempstead, Harvester Wheatsheaf.

Castells, M. (2006). La era de la información: economía, sociedad y cultura. Madrid, Alianza Editorial.

Comisión Nacional de los Mercados y la Competencia (CNMC). (2023). *Memoria 2023* [en línea]. Madrid, CNMC. [Consulta: 10 agosto 2025]. Disponible en: https://www.cnmc.es/sites/default/files/editor_contenidos/CNMC/Memorias/Memoria%20CNMC_2023.pdf

—. (2025). Unidad de Inteligencia Económica (UIE) [en línea]. [Consulta: 27 julio 2025]. Disponible en: https://www.cnmc.es/vigilamos-la-competencia/unidad-de-inteligencia-economica

Consejo de la Unión Europea. (2010). Estrategia de seguridad interior de la Unión Europea. Hacia un modelo europeo de

seguridad [en línea]. Luxemburgo, Consejo de la Unión Europea, Secretaría General, Oficina de Publicaciones. [Consulta: 12 agosto 2025]. Disponible en: https://data.europa.eu/doi/10.2860/881

—. (2020). Estrategia de la UE sobre drogas 2021–2025 [en línea]. Bruselas, Consejo de la Unión Europea, Secretaría General. [Consulta: 8 agosto 2025]. Disponible en: https://www.consilium.europa.eu/media/54074/qc0521073esn_002.pdf

Damro, C. (2012). Market power Europe [en línea]. Journal of European Public Policy. 19(5), pp. 682-699. [Consulta: 2026]. Disponible en: https://doi.org/10.1080/13501763.2011.646779

Davara Rodríguez, F. (2015). Planificación estratégica e inteligencia económica. *Cuadernos de estrategia*. N.º 174, pp. 189-229.

Departamento de Seguridad Nacional (DSN). (2013). Estrategia de Seguridad Marítima Nacional 2013 [en línea]. Departamento de Seguridad Nacional, Presidencia del Gobierno. [Consulta: 18 julio 2025]. Disponible en: https://www.lamoncloa.gob.es/documents/20131333estrategiadeseguridadmartima_u.pdf

—. (2017). Estrategia de Seguridad Nacional 2017 [en línea]. [Consulta: 7 julio 2025]. Disponible en: https://www.dsn.gob.es/es/buscador?key=Estrategia+de+Seguridad+Nacional+2017

—. (2021). Estrategia de Seguridad Nacional 2021 [en línea]. Departamento de Seguridad Nacional, Presidencia del Gobierno. [Consulta: 29 julio 2025]. Disponible en: https://www.dsn.gob.es/es/publicaciones/estrategia-de-seguridad-nacional-2021

—. (2024). Estrategia Nacional de Seguridad Marítima 2024 [en línea]. Departamento de Seguridad Nacional, Presidencia del Gobierno. [Consulta: 2026]. Disponible en: https://www.dsn.gob.es/es/publicaciones/estrategias-sectoriales/ENSM2024

Díaz Fernández, A. M. (2013). El papel de la inteligencia estratégica. *Cuadernos de estrategia*. N.º 162, pp. 35-66.

EMCDDA y Europol. (2024). EU Drug Markets Analysis: Key insights for policy and practice [en línea]. Luxemburgo, Publications Office of the EU. [Consulta: 25 agosto 2025]. Disponible

en: https://www.euda.europa.eu/publications/eu-drug-markets/analysis-key-insights-policy-and-practice_en

España. (1986). Ley Orgánica 2/1986, de 13 de marzo, de Fuerzas y Cuerpos de Seguridad [en línea]. Boletín Oficial del Estado. 3 de abril, núm. 63. [Consulta: 2026]. Disponible en: https://www.boe.es/buscar/act.php?id=BOE-A-1986-6859

—. (2002). Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia [en línea]. Boletín Oficial del Estado. 7 de mayo, núm. 109. [Consulta: 2026]. Disponible en: https://www.boe.es/buscar/act.php?id=BOE-A-2002-8628

—. (2010). Ley Orgánica 5/2010, de 22 de junio, por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal. [en línea]. Boletín Oficial del Estado. 23 de junio, núm. 152, pp. 54811-54883. [Consulta: 2026]. Disponible en: https://www.boe.es/eli/es/lo/2010/06/22/5

—. (2015). Ley 36/2015, de 28 de septiembre, de Seguridad Nacional. [en línea]. Boletín Oficial del Estado. 29 de septiembgre, núm. 233, pp. 87106-87117. [Consulta: 2026]. Disponible en: https://www.boe.es/buscar/doc.php?id=BOE-A-2015-10389

—. (2017). Real Decreto 1008/2017, de 1 de diciembre, por el que se aprueba la Estrategia de Seguridad Nacional 2017 [en línea]. Boletín Oficial del Estado. 22 de diciembre, núm. 309. [Consulta: 2026]. Disponible en: https://www.boe.es/buscar/act.php?id=BOE-A-2017-15181

—. (2019a). Orden PCI/161/2019, de 21 de febrero, por la que se publica el Acuerdo del Consejo de Seguridad Nacional, por el que se aprueba la Estrategia Nacional contra el Crimen Organizado y la Delincuencia Grave [en línea]. Boletín Oficial del Estado. 22 de febrero, núm. 46, pp. 17048-17074. [Consulta: 2026]. Disponible en: https://www.boe.es/eli/es/o/2019/02/21/pci161

—. (2019b). Orden PCI/487/2019, de 26 de abril, por la que se publica la Estrategia Nacional de Ciberseguridad 2019, aprobada por el Consejo de Seguridad Nacional [en línea]. Boletín Oficial del Estado. 30 de abril, núm. 103, pp. 43437-43455. [Consulta: 6 julio 2025]. Disponible en: https://www.boe.es/buscar/doc.php?id=BOE-A-2019-6347

—. (2021a). Real Decreto 1150/2021, de 28 de diciembre, por el que se aprueba la Estrategia de Seguridad Nacional 2021 [en línea]. Boletín Oficial del Estado. 31 de diciembre, núm. 314,

pp. 167795-167830. [Consulta: 2026]. Disponible en: https://www.boe.es/diario_boe/txt.php?id=BOE-A-2021-21884

—. (2021b). Resolución de 13 de enero de 2021, de la Presidencia de la AEAT, sobre organización y atribuciones de funciones en el Área de Aduanas e Impuestos Especiales [en línea]. Boletín Oficial del Estado. 15 de enero, núm. 13, pp. 3826-3850. [Consulta: 2026]. Disponible en: https://www.boe.es/eli/es/res/2021/01/13/(5)

—. (2024). Real Decreto 207/2024, de 27 de febrero, por el que se desarrolla la estructura orgánica básica del Ministerio del Interior. [en línea]. Boletín Oficial del Estado. 28 de febrero, núm. 52, pp. 23452-23487. [Consulta: 2026]. Disponible en: https://www.boe.es/diario_boe/txt.php?id=BOE-A-2024-3793

Esteban Navarro, M. Á. (2007). *Glosario de inteligencia*. Madrid, Ministerio de Defensa.

Eurojust. (2022). Eurojust Report on Money Laundering [en línea]. La Haya, Eurojust. [Consulta: 26 agosto 2025]. Disponible en: https://www.eurojust.europa.eu/publication/eurojust-report-money-laundering

—. (2025). Informe anual 2024 (ES) [en línea]. La Haya, Eurojust. [Consulta: 26 agosto 2025]. Disponible en: https://www.eurojust.europa.eu/about-us/planning-and-reporting/annual-report

European Commission et al. (2024). VAT gap in the EU: 2024 report [en línea]. Luxemburgo, Publications Office of the EU. [Consulta: 26 agosto 2025]. Disponible en: https://doi.org/10.2778/2476549

European Commission. (2024). Advancing European economic security: an introduction to five new initiatives [en línea]. [Consulta: 11 agosto 2025]. Disponible en: https://place-based-innovation.ec.europa.eu/publications/advancing-european-economic-security-introduction-five-new-initiatives_en

European Public Prosecutor's Office (EPPO). (2025). Annual Report 2024 [en línea]. Luxemburgo, Publications Office of the EU. [Consulta: 26 agosto 2025]. Disponible en: https://doi.org/10.2927/9973133

European Union Drugs Agency (EUDA). (2025). European Drug Report 2025: Trends and Developments [en línea]. Lisboa, European Union Drugs Agency (EUDA). [Consulta: 25 agosto

2025]. Disponible en: https://www.euda.europa.eu/publications/european-drug-report/2025_en

Europol. (2011). EU Organised Crime Threat Assessment (OCTA) 2011 [en línea]. [Consulta: 8 julio 2025]. Disponible en: https://www.Europol.europa.eu/publications-events/main-reports/octa-2011-eu-organised-crime-threat-assessment

—. (2013). European Union Serious and Organised Crime Threat Assessment (SOCTA) 2013 [en línea]. [Consulta: 23 agosto 2025]. Disponible en: https://op.europa.eu/en/publication-detail/-/publication/aecc0329-38b1-4a8c-9d92-a5c19044c420

—. (2017a). European Union Serious and Organised Crime Threat Assessment (SOCTA) 2017 [en línea]. [Consulta: 9 julio 2025]. Disponible en: https://data.europa.eu/data/datasets/serious-and-organised-crime-threat-assessment-2017

—. (2017b). From suspicion to action: converting financial intelligence into greater operational impact [en línea]. Luxemburgo, Publications Office of the EU. [Consulta: 20 julio 2025]. Disponible en: https://doi.org/10.2813/568228

—. (2021a). European Union Serious and Organised Crime Threat Assessment (SOCTA) 2021 [en línea]. [Consulta: 31 julio 2025]. Disponible en: https://op.europa.eu/en/publication-detail/-/publication/6e5575ce-c34b-11eb-a925-01aa75ed71a1

—. (2021b). Shadow money – the international networks of illicit finance. Europol Spotlight Series.

—. (2023). The other side of the coin: an analysis of financial and economic crime [en línea]. Luxemburgo, Publications Office. [Consulta: 14 agosto 2025]. Disponible en: https://data.europa.eu/doi/10.2813/105613

—. (2025). European Union Serious and Organised Crime Threat Assessment (EU SOCTA) 2025: The changing DNA of serious and organised-crime [en línea]. [Consulta: 12 julio 2025]. Disponible en: https://www.Europol.europa.eu/publication-events/main-reports/changing-dna-of-serious-and-organised-crime

FATF. (2012). Operational Issues: Financial Investigations Guidance. París, FATF.

—. (2022). Money Laundering from Fentanyl and Synthetic Opioids. París, FATF.

Friedman, T. L. (1999). *The Lexus and the Olive Tree: Understanding Globalization*. Nueva York, Farrar, Straus and Giroux.

HM Government. (2023). Serious and Organised Crime Strategy 2023-2028.

Jacques, M. (2012). *When China Rules the World*. 2.ª ed. Londres, Penguin.

Johnson, L. K. (2007a). *Handbook of Intelligence Studies*. Londres, Routledge.

—. (2017b). *National Security Intelligence*. Cambridge, Polity Press.

Kent, S. (1966). Strategic Intelligence for American World Policy [en línea]. Princeton, Princeton University Press. [Consulta: 31 agosto 2025]. Disponible en: https://www.jstor.org/stable/j.ctt183q0qt

LLYC. (2015). Inteligencia económica; una política pública para España [en línea]. Revista UNO. [Consulta: 11 julio 2025]. Disponible en: https://www.revista-uno.com/numero-19/inteligencia-economica-una-politica-publica-para-espana/

Lowenthal, M. M. (2012). *Intelligence: From Secrets to Policy*. Washington, DC, CQ Press.

McGann, J. G. (2020). *2019 Global Go To Think Tank Index Report*. Filadelfia, University of Pennsylvania.

Ministerio de Defensa. (2023). *Nuevas amenazas a la Seguridad Nacional*. Madrid, CESEDEN/ESFAS.

Nordhaus, W. D. (2013). The Climate Casino: Risk, Uncertainty, and Economics for a Warming World. New Haven, Yale University Press.

OECD y EUIPO. (2025). *Mapping Global Trade in Fakes 2025*. París/Alicante, OECD/European Union Intellectual Property Office (EUIPO).

Ruggie, J. G. (1992). Multilateralism: the Anatomy of an Institution. *International Organization*. 46(3), pp. 561-598.

SEPBLAC. (2024). *Memoria de actividades 2022–2023*. Madrid, SEPBLAC.

UNICRI. (2016). Organized Crime and the Legal Economy. Turín, UNICRI.

Weiss, L. (2014). America Inc.? Innovation and Enterprise in the National Security State. Ithaca, Cornell University Press.

Wendt, A. (1992). Anarchy is What States Make of It [en línea]. International Organization. 46(2), pp. 391-425. [Consulta: 2026]. Disponible en: https://www.jstor.org/stable/2706858

Wohlforth, W. C. (1999). The Stability of a Unipolar World. *International Security*. 24(1), pp. 5-41.