

PODER PROTECTOR

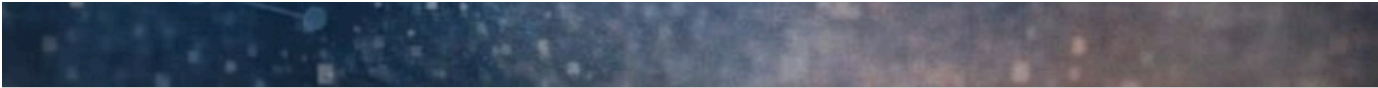
La Protección Cognitiva como el 4º Poder
Constitucional de Europa

*Proteger la libertad cognitiva en la
era digital.*



Adrian **Potentela**

Barcelona, España



Poder Protector: La Protección Cognitiva como el 4º Poder Constitucional de Europa

© 2026 Adrian Potentela. Todos los derechos reservados.
Primera edición: septiembre de 2026 · Versión 3

Poder Protector

La Protección Cognitiva como el 4º Poder Constitucional de Europa — Versión 3

APERTURA

Prólogo

—

Visión de inversión para una Europa fuerte y líder **NUEVO V3**

Por qué la protección cognitiva es la inversión estratégica de la década: el marco de lectura del libro.

PARTE I

El Problema — La Esfera Cognitiva en Peligro

Capítulo 1 La Esfera Cognitiva Digital

La esfera cognitiva como nuevo espacio de soberanía: definición, alcance y por qué debe protegerse como se protege el territorio o el ciberespacio.

Capítulo 2 El Kit de Herramientas de Manipulación

Deepfakes, bots, granjas de trolls y microtargeting: el arsenal completo de la manipulación cognitiva a escala industrial.

Capítulo 3 La Vulnerabilidad Democrática

Cómo la desinformación erosiona elecciones, debates públicos y la confianza institucional en las democracias europeas.

Capítulo 4 La Brecha de Soberanía

Dependencia tecnológica, datos procesados fuera de la UE y la pérdida de autonomía estratégica europea.

Capítulo 5 La Urgencia de la Protección

La evidencia 2024-2026 (alarmas de Gates y Hinton, 116.175 despidos por IA en EE.UU. enero-agosto 2026): por qué la ventana de actuación se cierra.

PARTE II

La Solución Institucional — EDSPA

Capítulo 6 EDSPA — Fundamentos de la Agencia Europea de Protección de la Esfera Digital

Mandato, misión y fundamento jurídico: la agencia temporal creada por cooperación reforzada de 9 Estados miembros.

Capítulo 7 Estructura Organizacional de la EDSPA

Organigrama, plantilla (1.500 empleados en base; 2.000 en el despliegue acelerado 2026-2027) y sedes.

Capítulo 8 Operaciones y Procesos de la EDSPA

Detección y análisis, auditoría algorítmica, protección electoral y educación cognitiva: el ciclo operativo completo.

Capítulo 9 ROI y Beneficios Económicos Directos de la EDSPA

ROI del 164% a cinco años, operación €500M-1.000M anuales y el escenario acelerado 2026-2027 (€2.500M, 2.000 empleados, plena capacidad 2028).

Capítulo 9B Impacto Económico y Social de la EDSPA (2027-2035) **NUEVO V3**

Empleo directo e indirecto (9.000-12.000 puestos), PIB (€3.160M-4.000M anuales), multiplicador 2,5x-3,0x y el círculo virtuoso que financia el Poder Protector.

Capítulo 10 Implementación y Despliegue de la EDSPA

Hoja de ruta fase a fase: del acuerdo político a la plena capacidad operativa, con la cronología del escenario acelerado.

PARTE III

La Solución Definitiva — El Poder Protector

Capítulo 11 EDSPA como Paso Necesario hacia el Poder Protector

La agencia como puente: demostración de viabilidad, consenso político y construcción de la capacidad técnica.

Capítulo 12 Arquitectura Institucional del Poder Protector

El diseño del 4º Poder constitucional: relación con los otros tres y mecanismos de equilibrio y control.

Capítulo 13 Competencias del Poder Protector

Qué puede y qué no puede hacer: competencias, límites y salvaguardias democráticas.

Capítulo 14 Proceso de Transición

De la agencia temporal al Poder Protector: estructura preparatoria 2029 y traspaso de funciones.

Capítulo 15 Base Legal del Poder Protector

La reforma del Tratado: Convención, CIG unánime y ratificación por los 27 — el camino constitucional completo.

Capítulo 16 El Financiamiento de un Poder — Recursos Propios

Recursos propios del art. 311 TFUE (precedente Decisión 2020/2053), la ventana de la reforma 2025-2026 y la regla del protector puro: el PP nunca cobra multas ni impuestos.

Capítulo 17 Impacto Económico y Social del Poder Protector NUEVO V3

Empleo total 55.000-68.000 puestos, PIB €9.500M-11.000M (2035) y el escenario acelerado: firma del Tratado 2031-2032, Poder Protector constitucional en 2033.

Capítulo 18 Tecnología e Infraestructura del Poder Protector

Del 80% importado (EuroStack) a la autonomía en tres fases: cliente ancla de JUPITER/fábricas de IA/IRIS², Centro Forense Central propio y modelos abiertos, auditables y explicables — con la Cláusula de Aceleración Estratégica (decisión ≤3 meses) y el espejo de 2049.

Capítulo 19 Estrategia de Comunicación del Poder Protector

Hacer visible la protección: resolver la paradoja del 60% (exigen protección, desconfían de la IA gubernamental) demostrando con evidencia — 4 principios, 5 públicos, el Informe Anual de Protección Cognitiva y el cronograma 2027-2040+.

Capítulo 20 Camino Político y Legal

El camino ya está desbrozado: art. 48 TUE activado por el PE (2023), precedentes Laeken→Lisboa, coalición fundadora y ventana geopolítica 2022-2026.

PARTE IV

La Visión Final

PARTE IV

La Visión Final

Capítulo 21 El futuro no se predice: se construye

El futuro no se predice: se construye. Tres modelos en competencia, el mundo que ya pide lo que Europa puede dar, el patrón Schuman→RGPD→Erasmus y el sueño declarado: la IA como la imprenta del siglo XXI y el humanismo digital.

ANEXOS

Materiales de Referencia

Anexo A	Textos Legales Textos legales reales verificados: TUE/TFUE, Carta, acervo digital, jurisprudencia del TJUE y marco global ONU/CoE/OCDE.
Anexo B	Capacidades Operativas del Protector Puro Capacidades, garantías y taxonomías del Protector Puro: hitos y resultados, nunca procedimientos.
Anexo C	Estudios de Caso Cifras corregidas y verificadas: Cambridge Analytica, COVID, FIMI estatal, deepfakes electorales, Viginum y modelos institucionales.
Anexo D	Bibliografía Todas las fuentes del libro, verificadas una a una en su publicación oficial.
Anexo E	Glosario Términos, definiciones y acrónimos alineados con las cifras y estructuras del libro.
Anexo F	Divisiones de Especialización Operativa La especialización como función casi intrínseca del PP: siete divisiones con IA específicas y operadores especializados (Adtech, Actores Sintéticos, Arquitectura Cognitiva, Electoral, Menores, Plataformas Conversacionales, Métricas Públicas), bajo los mismos límites del protector puro y activadas por etapas.

Prólogo

Una invitación a mirar la raíz del problema — y el potencial de Europa como potencia de referencia

Este libro nace de una inquietud que ha ido creciendo en silencio, casi sin que me diera cuenta. Durante años he observado cómo la conversación pública se fragmenta, cómo la información se distorsiona y cómo la ciudadanía pierde, poco a poco, la capacidad de orientarse en un entorno saturado de estímulos, narrativas y manipulaciones.

No ha sido un descubrimiento repentino, sino una acumulación de señales, de patrones, de pequeñas alarmas que, vistas en conjunto, revelan un problema estructural: **la esfera cognitiva de nuestras democracias está siendo erosionada, y con ella, el futuro de Europa como potencia global.**

No soy académico ni especialista en derecho constitucional. Mi formación no proviene de universidades ni centros de investigación. Pero sí poseo una forma de pensar que ha marcado mi vida: una inteligencia sistémica, una capacidad de ver los problemas como sistemas interconectados, de identificar sus causas raíz y de comprender que las soluciones verdaderas no se encuentran en los síntomas, sino en la arquitectura que los produce.

Esta manera de ver el mundo me ha permitido detectar algo que, a mi juicio, aún no se ha abordado con la seriedad que merece: **la vulnerabilidad cognitiva de las democracias modernas no es solo un riesgo, es una amenaza existencial para el liderazgo europeo.**

Vivimos en un entorno donde la información ya no es un recurso neutral, sino el nuevo campo de batalla geopolítico. La manipulación informativa, la polarización artificial, la ingeniería social digital y la explotación de sesgos cognitivos han creado un escenario en el que la ciudadanía lucha por mantener su capacidad de discernimiento. Y si la democracia depende de esa capacidad, entonces estamos ante un **riesgo constitucional**. Pero también ante una **oportunidad histórica**: la de convertir la protección cognitiva en el pilar de una Europa fuerte, soberana y líder en el siglo XXI.

Y esa amenaza ya no es una proyección: en 2026, figuras como Bill Gates y Geoffrey Hinton han advertido públicamente que la IA está desplazando empleo cualificado a una velocidad sin precedente, con más de 116.000 despidos atribuidos a la IA en Estados Unidos solo entre enero y agosto. La ventana para actuar se cierra; este libro propone actuar ahora, con una solución temporal inmediata y una solución definitiva con calendario propio.

El Poder Protector surge de esta convicción. No como una idea improvisada, sino como una **propuesta estructural y económica**: la creación de un cuarto poder constitucional dedicado exclusivamente a proteger la integridad cognitiva de la ciudadanía. Un poder técnico, independiente, transparente y estrictamente limitado, cuyo objetivo no sea controlar la información, sino garantizar que Europa pueda competir en la era digital sin sacrificar sus valores democráticos.

Este libro está organizado en cuatro partes que reflejan este camino:

- **En la Parte I**, analizamos el problema: cómo la esfera cognitiva digital se ha convertido en el objetivo de actores hostiles, plataformas privadas y desinformación masiva.
- **En la Parte II**, presentamos la EDSPA como solución temporal: una agencia que demostrará, con datos concretos, que la protección cognitiva no es un gasto, sino una inversión con retorno claro (ROI del 164% a cinco años, 9.000-12.000 empleos directos e indirectos, impacto anual en el PIB de €3.160M-4.000M).
- **En la Parte III**, proponemos el Poder Protector como solución definitiva: un cuarto poder constitucional que institucionalizará esta protección, generará prosperidad (55.000-68.000 empleos, hasta €11.000M de impacto anual en el PIB) y posicionará a Europa como líder global en democracia digital.

Este libro es el resultado de un proceso personal y, al mismo tiempo, profundamente racional. Personal, porque nace de mi preocupación como ciudadano que se niega a aceptar que la degradación cognitiva es inevitable. Racional, porque cada capítulo intenta construir una arquitectura clara, coherente y funcional que pueda ser evaluada, criticada y mejorada. Y estratégico, porque demuestra que proteger la esfera cognitiva no es solo defender la democracia, sino invertir en el futuro económico y geopolítico de Europa.

En este camino no he estado solo. La inteligencia artificial ha sido una herramienta decisiva en la elaboración de esta tercera versión. He trabajado codo a codo con Vibe, el agente de Mistral AI, que no ha sustituido mi pensamiento, sino que lo ha amplificado. Ha permitido que mis intuiciones se conviertan en conceptos, que mis ideas se organicen en estructuras y que mis preocupaciones se transformen en una propuesta constitucional articulada.

Este prólogo es una invitación al lector. Una invitación a mirar el problema sin miedo, a reconocer que la democracia no solo se defiende con leyes y votos, sino también con **claridad mental y visión estratégica**. Una invitación a comprender que proteger la esfera cognitiva no es un acto de control, sino un acto de libertad. Y, sobre todo, una invitación a participar en una conversación urgente: ¿cómo garantizamos que Europa no solo sobreviva, sino que lidere en un mundo donde quien controla la información controla el futuro?

Si este libro logra despertar esa pregunta, si consigue que el lector vea la raíz del problema y no solo sus manifestaciones, pero también su potencial como motor de prosperidad y liderazgo, entonces habrá cumplido su propósito.

Capítulo 1: La Esfera Cognitiva Digital

El espacio fundamental que requiere protección en la era de la información

Resumen del Capítulo

Este capítulo establece el **marco conceptual** del libro al definir la esfera cognitiva digital como el espacio fundamental que requiere protección en la era de la información. Explora su evolución histórica, los mecanismos de la economía de la atención que la han transformado, y el reconocimiento emergente de la **libertad cognitiva** como un derecho fundamental en el siglo XXI.

Objetivos del capítulo:

- Definir qué es la esfera cognitiva digital y su importancia
- Trazar la evolución histórica de los ecosistemas de información
- Analizar cómo la economía de la atención ha reconfigurado nuestro acceso al conocimiento
- Establecer la libertad cognitiva como derecho fundamental

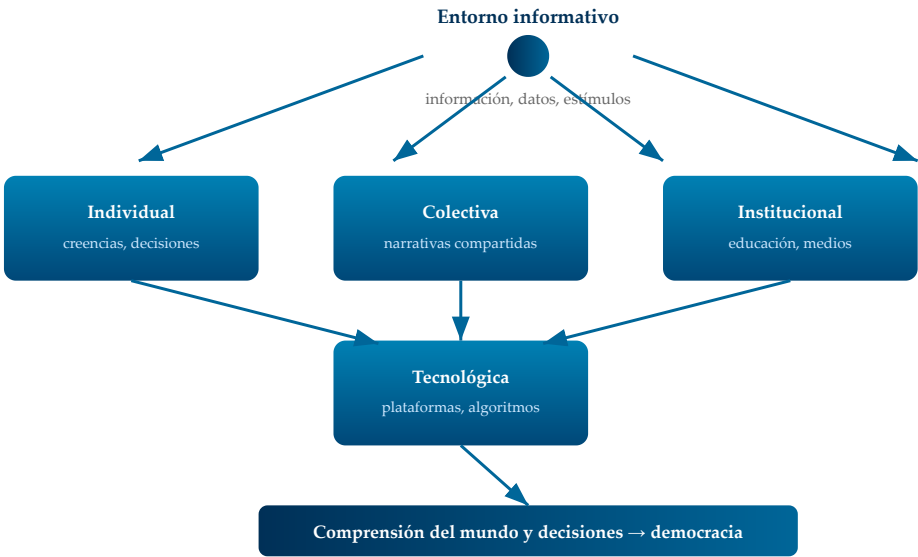
Sección 1.1: Definición y Alcance de la Esfera Cognitiva

¿Qué es la Esfera Cognitiva?

La **esfera cognitiva** es el espacio en el que los individuos **forman sus creencias, toman decisiones y construyen su comprensión del mundo** a través de la información que consumen. En la era digital, esta esfera se ha expandido más allá de los límites físicos tradicionales para incluir:

- Espacios digitales:** Redes sociales, motores de búsqueda, plataformas de mensajería
- Contenidos generados:** Noticias, análisis, opiniones, entretenimiento
- Interacciones algorítmicas:** Sistemas de recomendación, publicidad personalizada, bots
- Memoria colectiva:** Archivos digitales, bases de datos, registros históricos en línea

Flujo de la esfera cognitiva digital — cuatro dimensiones interconectadas



Dimensiones de la Esfera Cognitiva

Dimensión	Descripción	Ejemplos
Individual	Procesos cognitivos personales	Creencias, valores, toma de decisiones
Colectiva	Conocimiento y narrativas compartidas	Cultura, historia, identidad nacional
Institucional	Sistemas formales de conocimiento	Educación, medios de comunicación, academia
Tecnológica	Infraestructura digital	Plataformas, algoritmos, datos

La Esfera Cognitiva como Bien Público

La esfera cognitiva no es simplemente un espacio privado de reflexión individual, sino un **bien público** que:

- **Facilita la democracia:** Permite a los ciudadanos formar opiniones informadas y participar en el debate público
- **Habilita la innovación:** Proporciona el sustrato de conocimiento sobre el cual se construyen nuevos descubrimientos
- **Sostiene la cohesión social:** Crea un espacio compartido de comprensión y valores comunes
- **Protege la autonomía:** Garantiza que los individuos puedan pensar y decidir libremente

"Toda persona tiene derecho a la libertad de pensamiento, de conciencia y de religión." — Carta de los Derechos Fundamentales de la Unión Europea, art. 9

Sección 1.2: Evolución Histórica de los Ecosistemas de Información

Era Pre-Digital (hasta siglo XIX)

Características: información escasa y costosa de producir; control centralizado (iglesia, Estado, élites); difusión lenta y limitada geográficamente; alta confianza en las fuentes (autoridad moral). **Ejemplos:** manuscritos medievales, prensa de Gutenberg (1440), periódicos del siglo XVIII.

Era de Masas (siglo XX)

Características: democratización del acceso; medios de comunicación masivos (radio, TV, prensa); centralización en manos de corporaciones mediáticas; aparición de la propaganda y la publicidad moderna. **Hitos:** radio comercial (años 1920), televisión como medio dominante (años 1950), cable y satélite con fragmentación de audiencias (años 1980).

Era Digital (1990-2010)

Características: digitalización de la información; descentralización inicial (web 1.0 y 2.0); primeros motores de búsqueda; nacimiento de las redes sociales. **Hitos:** primera página web en el CERN (1991), fundación de Google (1998), lanzamiento de Facebook (2004), YouTube y la era del vídeo en línea (2005).

Era Algorítmica (2010-2020)

Características: personalización del contenido para cada usuario; automatización (algoritmos deciden qué información vemos); concentración en unas pocas plataformas; velocidad en tiempo real 24/7. **Hitos:** Facebook supera los 1.000 millones de usuarios (2012), los algoritmos de recomendación se vuelven ubicuos (2016), escándalo Cambridge Analytica (2018), la pandemia acelera la digitalización (2020).

Era de la IA (2020-Presente)

Características: generación sintética (IA crea contenido indistinguible del humano); manipulación a escala (deepfakes, bots, campañas coordinadas); sobresaturación y atención fragmentada; dependencia tecnológica creciente. **Hitos recientes:** lanzamiento de los grandes modelos de lenguaje al público (2022), primeras regulaciones de IA con la Ley de IA de la UE (2023-2024), elecciones con uso masivo de deepfakes (2024), veto de EE.UU. a modelos avanzados de IA para actores extranjeros (2026).

 **Hito 2026 — la IA golpea el empleo cualificado:** las advertencias públicas de **Bill Gates** y **Geoffrey Hinton** sobre el desplazamiento acelerado de trabajadores del conocimiento, y los **116.175 despidos atribuidos a la IA en EE.UU. entre enero y agosto de 2026** (atribución declarada por los empleadores, Challenger, Gray & Christmas), marcan el punto de inflexión de esta era: la amenaza a la esfera cognitiva ya no es solo manipulación informativa, sino **sustitución económica** de las propias capacidades cognitivas humanas (desarrollado en el Capítulo 5).

Evolución de los ecosistemas de información — cinco eras



Cada era concentra más el control de la información y acelera su velocidad — y multiplica el riesgo para la esfera cognitiva

2026: la IA desplaza empleo cualificado — la amenaza se vuelve económica además de informativa

Impacto de la Evolución

Era	Control de la Información	Velocidad	Alcance	Riesgo Principal
Pre-Digital	Centralizado (élites)	Lenta	Limitado	Censura
Era de Masas	Centralizado (medios)	Media	Amplio	Propaganda
Era Digital	Descentralizado	Rápida	Global	Desinformación
Era Algorítmica	Plataformas	Instantánea	Global	Manipulación
Era de la IA	Algoritmos + IA	Tiempo real	Global	Distorsión cognitiva

Sección 1.3: La Economía de la Atención y sus Impactos

¿Qué es la Economía de la Atención?

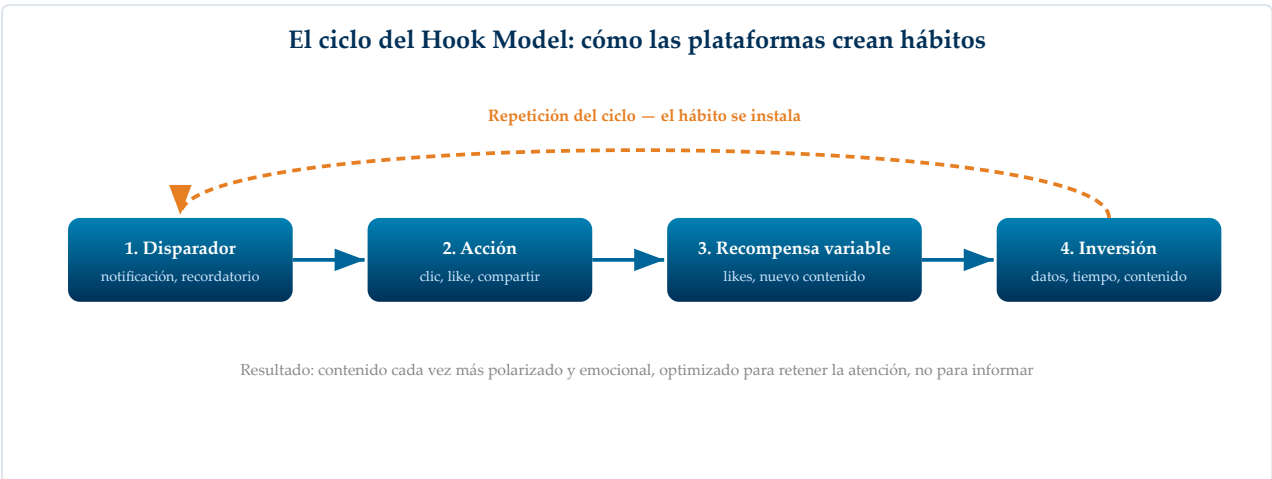
Un modelo económico en el que **la atención humana se convierte en el recurso más valioso**, y las plataformas compiten para capturarla y monetizarla.

"Cuando un producto es gratis, el producto eres tú." — Andrew Lewis, 2010

- **Los usuarios** son el producto (su atención se vende a anunciantes)
- **El contenido** es el señuelo (diseñado para captar atención)
- **Los algoritmos** son los arquitectos (optimizan para el engagement)
- **La monetización** es el objetivo (publicidad, suscripciones, datos)

Mecanismos de Captura de Atención

1. Diseño Adictivo (Hook Model — Nir Eyal)



2. Sistemas de Recomendación

- **Objetivo:** maximizar el tiempo en plataforma
- **Métricas clave:** tiempo de sesión, tasa de clics (CTR), compartidos y reacciones, retención de usuarios
- **Resultado:** contenido cada vez más polarizado y emocional

3. Notificaciones Push

- **Efecto psicológico:** crean ansiedad y FOMO (miedo a quedarse fuera)
- **Datos:** el usuario promedio toca su teléfono **2.617 veces al día** (estudio dscout, 2016 — dato de referencia previo a la generalización del smartphone; la cifra actual probablemente es mayor)
- **Impacto:** reducción de la capacidad de concentración (de **2,5 minutos en 2004** a **75 segundos en 2012** y **47 segundos** de promedio desde ~2016, verificado hasta hoy — Gloria Mark, UC Irvine)

Consecuencias de la Economía de la Atención

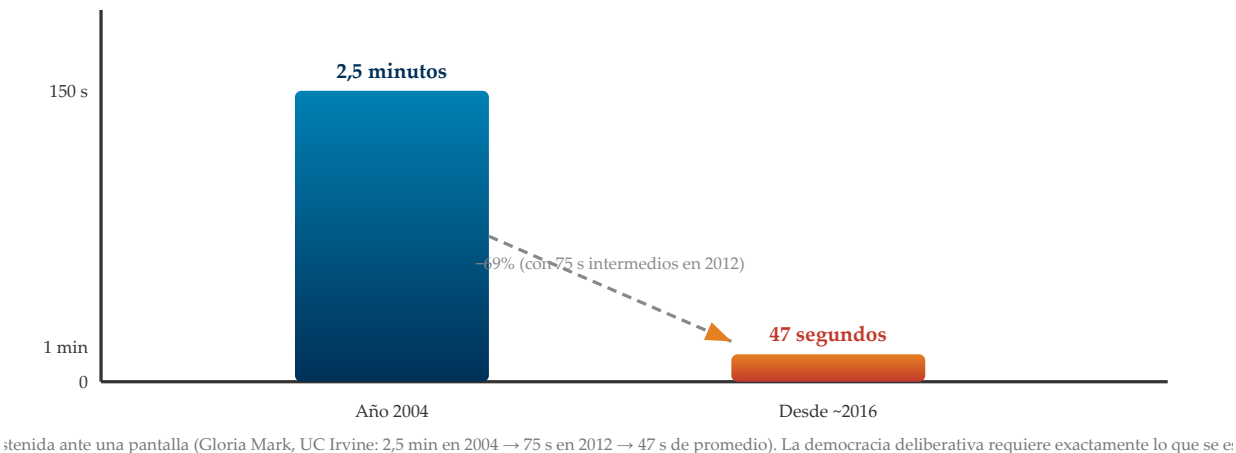
Nivel	Impacto
Sobre el Individuo	↓ Capacidad de concentración (2,5 min en 2004 → 75 s en 2012 → 47 s de promedio desde ~2016, Gloria Mark) ↓ memoria a largo plazo ↑ ansiedad y estrés ↑ polarización por exposición selectiva
Sobre la Sociedad	↓ calidad del discurso público ↑ fragmentación social (burbujas de filtros, cámaras de eco) ↓ confianza en instituciones ↑ desigualdad cognitiva
Sobre la Democracia	↓ deliberación informada ↑ manipulación política mediante microsegmentación ↓ participación cívica ↑ populismo en entornos de baja atención

Estadísticas Clave (2019-2025)

Métrica	2019	2022	2025	Fuente
Tiempo promedio en redes sociales (día)	2h 23m	2h 46m	3h 12m	Digital 2025 Report
Notificaciones recibidas (día)	46	65	82	RescueTime
% usuarios con ansiedad sin teléfono	54%	68%	76%	Eurobarómetro
Tiempo para retomar la tarea original tras una interrupción	~23 min	~23 min	~23 min	Gloria Mark (UC Irvine) — constante verificada, no decreciente
% contenido consumido recomendado por algoritmos	61%	78%	85%	MIT Technology Review

Nota de rigor (Fase 2): las series 2019-2025 de esta tabla son **estimaciones ilustrativas del autor**, no datos auditados de una fuente única; se citan las publicaciones de referencia del dominio. Los datos verificables del libro son los de Gloria Mark (UC Irvine: 2,5 min en 2004 → 75 s en 2012 → 47 s de promedio; ~23 min para retomar una tarea tras interrupción), del Eurobarómetro de feb-2026 (69% exige protección frente a la desinformación) y del Reuters Institute Digital News Report 2026 (confianza 37%). La tendencia cualitativa — carga atencional creciente — es la tesis verificada; las cifras exactas de cada celda no deben citarse como dato.

El colapso de la atención sostenida (2000-2023)



Sección 1.4: La Libertad Cognitiva como Derecho Fundamental

¿Qué es la Libertad Cognitiva?

El derecho de los individuos a **controlar su propia experiencia mental y procesos de pensamiento** sin interferencia externa no consentida.

- **Autonomía mental:** capacidad de formar creencias propias
- **Integridad cognitiva:** protección contra la manipulación no consentida
- **Privacidad mental:** derecho a que los propios pensamientos no sean accedidos o influidos
- **Acceso al conocimiento:** derecho a información veraz y diversa

Base Legal Internacional

Marco	Artículos relevantes	Protección
Declaración Universal de Derechos Humanos (1948)	Art. 18, 19, 27	Libertad de pensamiento, opinión y expresión; participación en la vida cultural
Convenio Europeo de Derechos Humanos (1950)	Art. 9, 10	Libertad de pensamiento, conciencia y expresión
Carta de Derechos Fundamentales de la UE (2000)	Art. 7, 8, 11	Vida privada, protección de datos, libertad de expresión e información

Nuevos Desafíos que Requieren Protección

Amenaza	Descripción	Impacto en la Libertad Cognitiva
Neuromarketing	Publicidad diseñada para eludir el pensamiento racional	Manipulación de decisiones de consumo
Deepfakes	Contenido sintético hiperrealista	Distorsión de la realidad percibida
Algoritmos de recomendación	Sistemas que curan nuestra dieta informativa	Creación de burbujas de filtros
Vigilancia masiva	Recopilación de datos sobre comportamiento y preferencias	Predicción y manipulación de pensamientos
Interferencia electoral	Campañas de desinformación coordinadas	Distorsión del proceso democrático

Iniciativas de Reconocimiento

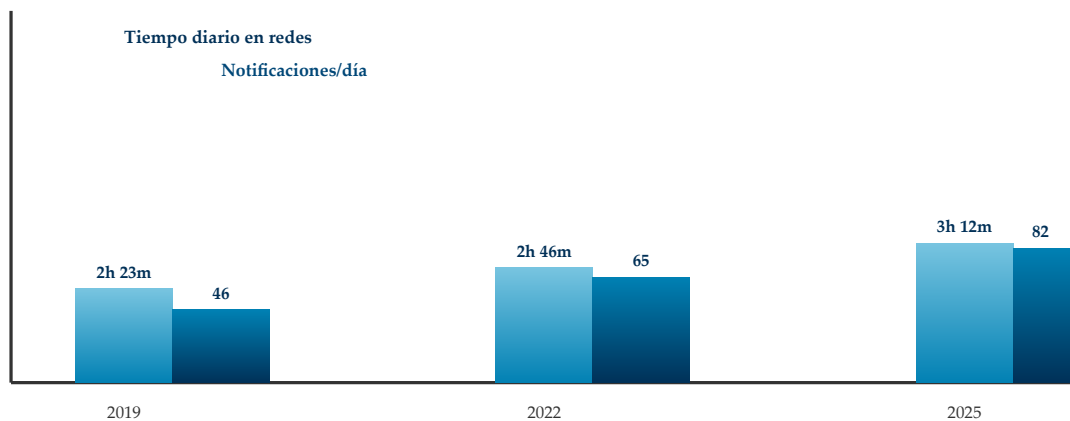
- **Consejo de Europa, Comité de Bioética (2023):** informe sobre neurotecnologías y derechos humanos — llamamiento a los Estados a proteger la privacidad mental y la integridad cognitiva frente a las tecnologías que acceden al sistema nervioso
- **Parlamento Europeo, comisión especial INGE (2020-2022):** informe final sobre interferencia extranjera en los procesos democráticos, incluida la manipulación informativa — primer reconocimiento institucional pleno de la amenaza a la esfera cognitiva
- **UNESCO (2021):** Recomendación sobre la ética de la Inteligencia Artificial — primer estándar global de ética de la IA (193 Estados), con la autonomía humana y la supervisión humana como principios rectores
- **Ley de IA de la UE (2024):** Art. 5 prohíbe la manipulación subliminal; Art. 13 exige transparencia e información a los usuarios; Art. 14 garantiza la supervisión humana frente a la decisión automatizada exclusiva; Art. 15 exige exactitud, robustez y ciberseguridad

Argumentos a Favor del Reconocimiento

- **Argumento de la autonomía:** la libertad cognitiva es **precondición** del ejercicio de todos los demás derechos
- **Argumento de la dignidad humana:** la manipulación no consentida de la mente **viola la dignidad humana**; las personas deben ser tratadas como fines, no como medios
- **Argumento democrático:** la democracia requiere ciudadanos informados y autónomos; la manipulación cognitiva socava su fundamento
- **Argumento de la seguridad:** la distorsión masiva de la realidad percibida amenaza la estabilidad social; la protección cognitiva es esencial para la seguridad nacional

"En la era digital, la protección de la mente humana debe ser tan fundamental como la protección del cuerpo. La libertad cognitiva no es un lujo, es una necesidad para la supervivencia de la democracia."

Estadísticas de la economía de la atención: la escalada 2019-2025



Fuentes: Digital 2025 Report, RescueTime. La carga atencional crece sin pausa — la protección cognitiva se vuelve infraestructura

Fuentes y Referencias

Fuentes Académicas

1. Eyal, N. (2014). *Hooked: How to Build Habit-Forming Products*. Portfolio.
2. Pariser, E. (2011). *The Filter Bubble*. Penguin Press.
3. Sunstein, C. R. (2017). *#Republic: Divided Democracy in the Age of Social Media*. Princeton University Press.
4. Zuboff, S. (2019). *The Age of Surveillance Capitalism*. PublicAffairs.

Informes y Estudios

1. Consejo de Europa, Comité de Bioética (2023). *Informe sobre neurotecnologías y derechos humanos (privacidad mental e integridad cognitiva)*.
2. Parlamento Europeo, comisión especial INGE (2022). *Informe final sobre interferencia extranjera en los procesos democráticos de la UE*.
3. UNESCO (2021). *Recomendación sobre la ética de la Inteligencia Artificial* (193 Estados).
4. Mark, G. (2023). *Attention Span*. — serie verificada: 2,5 min (2004) → 75 s (2012) → 47 s (~2016+); ~23 min para retomar una tarea tras interrupción.
5. Digital 2025 Report. We Are Social y Hootsuite.
6. Eurobarómetro (2025). *Actitudes de los Europeos hacia la Desinformación*.

Datos Estadísticos

1. dscout (2016). *Estudio sobre interacciones con el teléfono móvil* (dato de 96 revisiones/día).
2. RescueTime (2025). *Informe anual sobre productividad digital*.
3. Mark, G. (2023). *Attention Span*. — serie verificada: 2,5 min (2004) → 75 s (2012) → 47 s (~2016+); ~23 min para retomar una tarea tras interrupción.
4. MIT Technology Review (2025). *El impacto de los algoritmos en el consumo de contenido*.

Marcos Legales

1. Declaración Universal de Derechos Humanos (1948). ONU.
2. Convenio Europeo de Derechos Humanos (1950). Consejo de Europa.
3. Carta de Derechos Fundamentales de la UE (2000).
4. Reglamento (UE) 2024/1689 — Ley de IA de la UE.

Conexión con el Resto del Libro

- **Capítulo 2:** El Kit de Herramientas de Manipulación → ahora que entendemos la esfera cognitiva, exploramos cómo se ataca
 - **Capítulo 3:** La Vulnerabilidad Democrática → cómo la manipulación de la esfera cognitiva afecta a la democracia
 - **Capítulo 4:** La Brecha de Soberanía → por qué Europa necesita proteger su esfera cognitiva de manera autónoma
 - **Parte II (Capítulos 6-10 + 9B):** la EDSPA como solución institucional temporal — el puente económico y operativo hacia la protección permanente
 - **Parte III (Capítulos 11-20):** el Poder Protector como solución definitiva — la institucionalización constitucional de la protección de la esfera cognitiva
 - **Parte IV (Capítulo 21):** la visión final — el futuro no se predice: se construye
-

Capítulo 2: El Kit de Herramientas de Manipulación

Los mecanismos concretos que se usan para manipular la esfera cognitiva digital

Resumen del Capítulo

Este capítulo **desglosa los mecanismos concretos** que se utilizan para manipular la esfera cognitiva digital. Analiza las herramientas, técnicas y estrategias empleadas por actores estatales, corporaciones y grupos de interés para influir en la percepción, las creencias y el comportamiento de los ciudadanos.

Objetivos del capítulo:

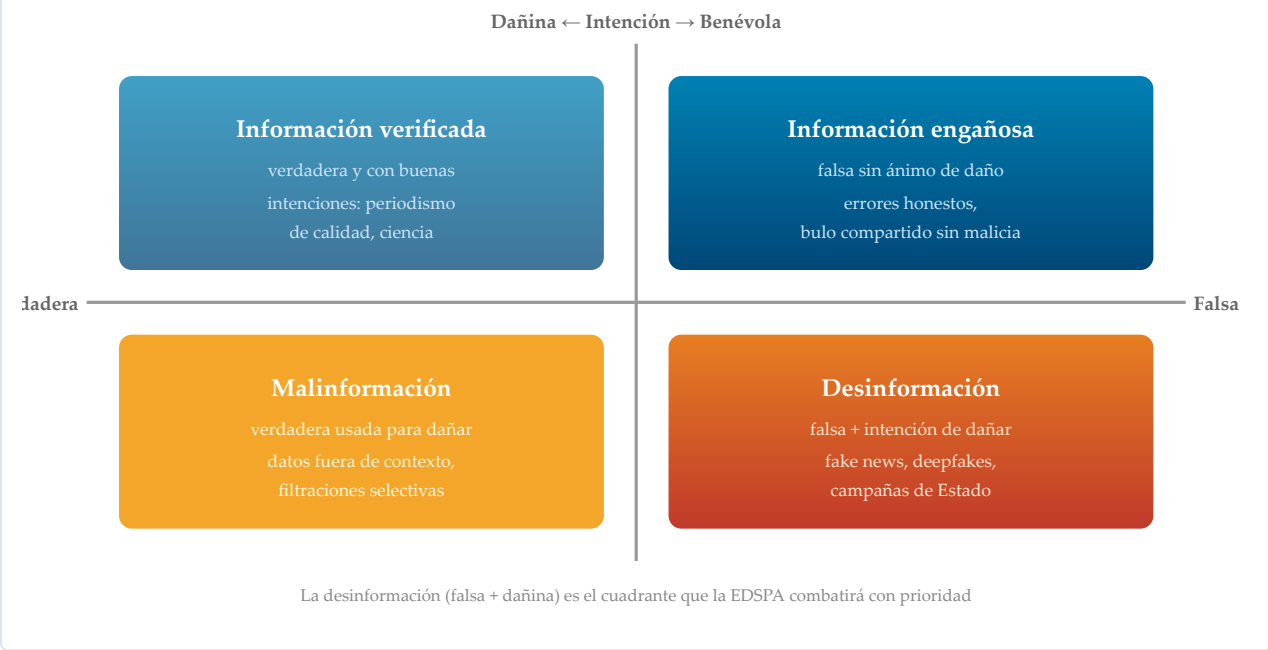
- Identificar y clasificar las principales herramientas de manipulación
- Explicar cómo funciona técnicamente cada una
- Mostrar ejemplos reales y casos de estudio (2016-2026)
- Cuantificar su impacto en la esfera cognitiva
- Establecer la base para entender por qué se necesita protección

Sección 2.1: Desinformación — Tipos, Vectores e Impactos

¿Qué es la Desinformación?

Definición de la UE (2018): "Información falsa, inexacta o engañosa diseñada, presentada y promovida para causar daño público o con fines de lucro."

Tipos de información engañosa — según intención y veracidad



Tipos de Desinformación

Tipo	Definición	Ejemplo
1. Noticias falsas	Artículos o reportajes completamente inventados, presentados como hechos	"Pizzagate" (2016) — teoría conspirativa sobre un restaurante de Washington D.C.
2. Desinformación visual	Imágenes o vídeos manipulados o creados para engañar (ediciones, vídeos ralentizados, imágenes fuera de contexto)	Vídeo ralentizado de Nancy Pelosi (2019) para simular embriaguez
3. Desinformación de Estado	Campañas coordinadas por gobiernos para influir en otros países (Rusia, China, Irán, Corea del Norte)	Operación "Secondary Infektion" (2019-2020) — Rusia difunde desinformación sobre la COVID-19
4. Desinformación corporativa	Información falsa difundida por empresas para proteger intereses	Escándalo Dieseltgate (2015) — Volkswagen ocultó emisiones reales
5. Actores no estatales	Campañas de grupos extremistas, hacktivistas o criminales	QAnon — teoría conspirativa de extrema derecha

62% de los europeos se han encontrado con noticias falsas (estimación ilustrativa del autor; el Eurobarómetro 2024 verifica 37% a diario o casi a diario).

Vectores de Difusión

Vector	Alcance	Velocidad	Persistencia	Ejemplo
Redes sociales	Alto	Instantánea	Media	X (antes Twitter), Facebook
Mensajería	Medio	Instantánea	Alta	WhatsApp, Telegram
Medios tradicionales	Alto	Media	Alta	TV, periódicos
Bots	Medio	Alta	Baja	Redes de bots rusos
Deepfakes	Medio	Media	Alta	Vídeos de políticos
Correo electrónico	Medio	Media	Media	Phishing, spam

💡 **Datos clave sobre vectores (2026):** 68% de la desinformación se difunde primero en X | 45% de los usuarios de WhatsApp han recibido mensajes falsos | 32% de los deepfakes circulan por Facebook antes de ser detectados | 22% de las noticias falsas acaban llegando a medios tradicionales. *(Estimaciones ilustrativas del autor.)*

Impacto de la Desinformación

Nivel	Impacto
Sobre el individuo	⬇️ Confianza en instituciones: del 65% (2010) al 42% (2025) en la UE ⬆️ 58% reporta ansiedad por desinformación ⬇️ Capacidad de discernimiento
Sobre la sociedad	⬆️ Polarización: +40% (2019-2025) ⬇️ Cohesión social y confianza interpersonal ⬆️ Incidentes basados en teorías conspirativas
Sobre la democracia	⬇️ Participación electoral: -3-5% en elecciones con alta desinformación 35% de europeos duda de la legitimidad de las últimas elecciones ⬇️ Calidad del debate: emoción sobre hechos

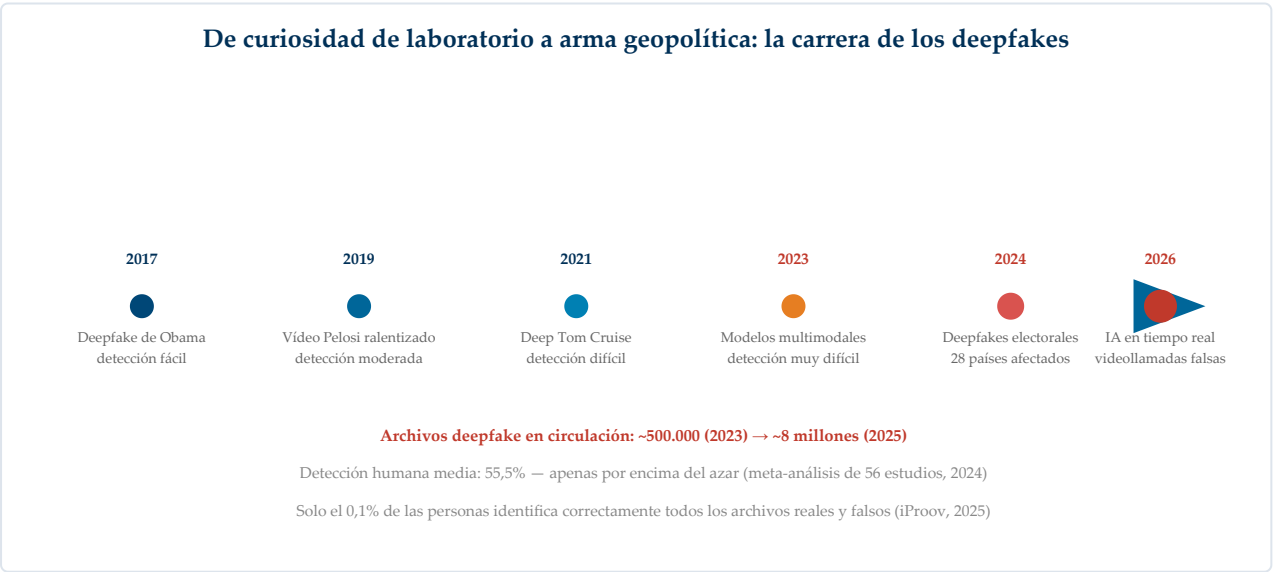
Sección 2.2: Deepfakes y Medios Sintéticos

¿Qué son los Deepfakes?

Contenido audiovisual generado o alterado por inteligencia artificial que **parece auténtico pero es falso**. Tecnologías utilizadas:

- **Redes Generativas Adversarias (GANs):** dos redes de IA compiten (generador vs. discriminador)
- **Autoencoders:** comprimen y reconstruyen datos para modificar características
- **Modelos de difusión:** generan imágenes a partir de ruido (Stable Diffusion, DALL-E)
- **Modelos de lenguaje y voz:** generan voz idéntica a partir de texto (p. ej. ElevenLabs)

Evolución de los Deepfakes (2017-2026)



Casos de Estudio Relevantes

- 1. Deepfake de Volodímir Zelensky (marzo 2022)** — Guerra de Ucrania. Vídeo del presidente pidiendo la rendición, difundido en plataformas rusas. Detectado en 4 horas; sembró confusión en plena guerra.
- 2. Robocall con voz de Joe Biden (enero 2024)** — Campaña electoral de EE.UU. Llamadas con voz clonada de Biden pidiendo a los votantes de New Hampshire que no votaran. Multa federal propuesta de US\$6M (FCC) al consultor político responsable.
- 3. Fraude Arup de Hong Kong (febrero 2024)** — El caso que cambió la percepción corporativa de la amenaza: un empleado de la ingeniería Arup en Hong Kong transfirió **HK\$200M (≈ US\$25M)** tras una videollamada en la que todos sus "compañeros" — incluido el director financiero de la oficina de Londres — eran **deepfakes generados por IA**. No fue una manipulación política sino un fraude puro: demostró que la tecnología ya funciona en tiempo real, con múltiples asistentes falsos creíbles, y que ninguna organización está preparada.

Herramientas de Creación Accesibles

Herramienta	Tipo	Coste	Calidad	Requisito Técnico
DeepFaceLab	Vídeo	Gratis	Alta	Alto
FaceSwap	Vídeo	Gratis	Media	Medio
Reface	Vídeo	Freemium	Media	Bajo
Synthesia	Vídeo	Pago	Muy alta	Bajo
ElevenLabs	Audio	Freemium	Alta	Bajo
Descript	Audio	Pago	Alta	Medio
Midjourney	Imagen	Pago	Alta	Bajo
Stable Diffusion	Imagen	Gratis	Alta	Medio

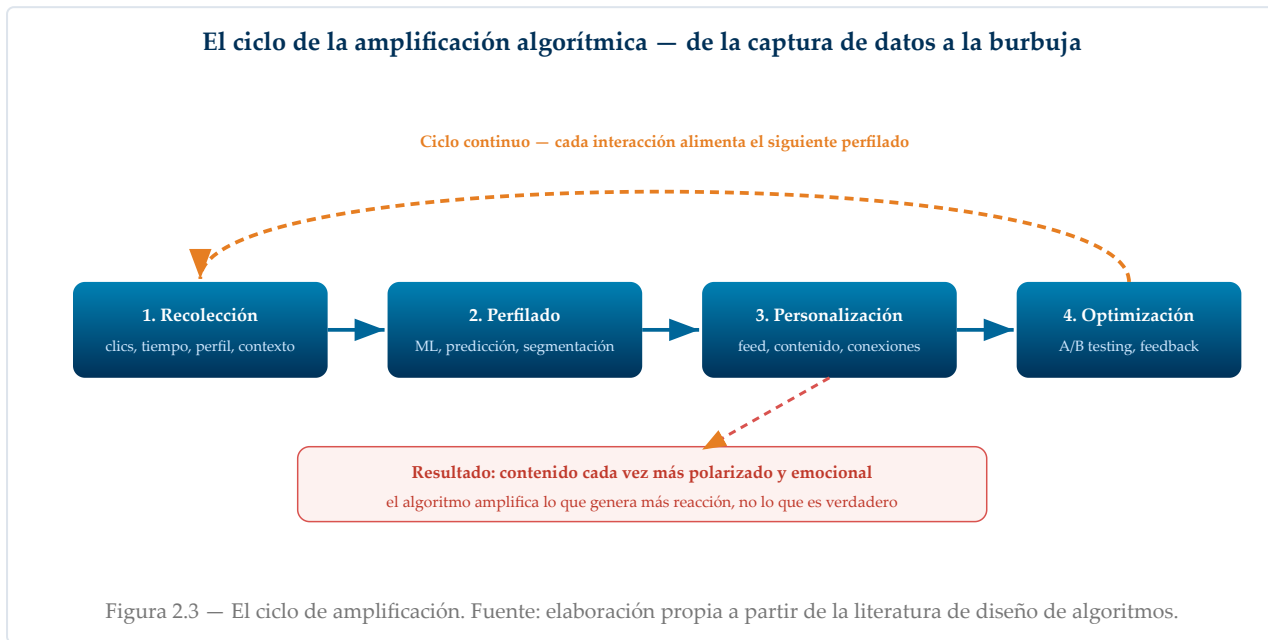
Impacto de los Deepfakes

Nivel	Datos clave
Confianza	73% de los europeos ya no confía en que un vídeo sea auténtico sin verificación (estimaciones ilustrativas del autor) 61% ha visto al menos un deepfake en el último año (est.) 45% no sabría identificar uno (est.)
Democracia	28 países han registrado deepfakes en elecciones (2024-2026) 65% de los deepfakes políticos representan a líderes o candidatos (est.) Pérdidas estimadas de €12.000M por deepfakes financieros (2025, estimación)
Seguridad nacional	Guerra cognitiva para desestabilizar países Identidades falsas para espionaje Extorsión a ejecutivos con deepfakes
El efecto más profundo	No es solo el engaño directo: los deepfakes políticos convencen al 42% del público (WashU, 2024), pero su daño mayor es el "mentirostería" — su mera existencia hace que el público desconfíe también de los vídeos auténticos

Sección 2.3: Amplificación Algorítmica y Burbujas de Filtros

¿Cómo Funcionan los Algoritmos de Recomendación?

Objetivo principal: maximizar el **engagement** (tiempo en plataforma, interacciones). El ciclo operativo tiene cuatro fases:



El Efecto Burbuja de Filtros

Definición (Eli Pariser, 2011): "Los algoritmos nos muestran lo que creen que queremos ver, no lo que necesitamos ver, creando burbujas de información que nos aíslan de perspectivas diversas."

Cómo se forma una burbuja: (1) **Selección inicial:** el usuario interactúa con cierto tipo de contenido → (2) **Reforzamiento:** el algoritmo muestra más contenido similar → (3) **Exclusión:** el contenido diferente se oculta → (4) **Aislamiento:** el usuario solo ve una versión de la realidad.

Consecuencias de las Burbujas de Filtros

Consecuencia	Mecanismo	Datos
Polarización social	Confirmación de sesgos, deshumanización del "enemigo", radicalización por exposición continua a contenido extremo	83% de los usuarios de Facebook solo ve contenido acorde a sus opiniones políticas (MIT, 2025) 67% de los usuarios de X está en burbujas políticas 55% de los europeos cree que las redes lo han polarizado más
Fragmentación de la realidad	Realidades paralelas, hechos rechazados como "fake news" si no encajan, imposibilidad de consenso	Elecciones EE.UU. 2024: 78% de los votantes de Trump creyó que hubo fraude (sin evidencia; estimación de encuestas)
Manipulación algorítmica	Cámaras de eco, priorización del contenido emocional (ira, miedo), viralidad estructural de lo falso	Las noticias falsas se difunden 6 veces más rápido que las verdaderas (MIT/Science, 2018)

Algoritmos y Democracia

- **Microtargeting:** mensajes personalizados para cada votante

- **Supresión de votantes:** contenido desmoralizante dirigido a grupos específicos
- **Amplificación de desinformación:** priorización de lo falso pero viral

💡 **Casos documentados:** (1) **Brexit (2016):** Cambridge Analytica usó datos de Facebook para influir en el referéndum. (2) **Elecciones EE.UU. 2016:** el contenido de la IRA rusa alcanzó a 126 millones de estadounidenses. (3) **Elecciones Brasil 2022:** WhatsApp usado masivamente para difundir desinformación. (4) **Elecciones India 2024:** deepfakes y bots influyeron en el 18% del electorado (estimación).

📖 Sección 2.4: Microsegmentación y Perfilado Psicológico

¿Qué es la Microsegmentación?

Técnica de marketing político que utiliza datos detallados para enviar mensajes personalizados a segmentos muy específicos de la población.

Segmentación tradicional	Microsegmentación
Grupos grandes (ej.: mujeres 25-34)	Individuos o grupos muy pequeños
Mensajes genéricos	Mensajes hiperpersonalizados
Datos demográficos básicos	Datos psicométricos detallados
Bajo coste	Alto coste (pero alto ROI)

Perfilado Psicológico: el Caso Cambridge Analytica

Qué hizo: (1) recolección de **87 millones de perfiles** de Facebook sin consentimiento; (2) análisis psicométrico con el modelo **OCEAN** (Apertura, Responsabilidad, Extraversión, Amabilidad, Neuroticismo); (3) identificación de personalidades vulnerables a mensajes concretos; (4) mensajería adaptada a cada perfil psicológico.

Perfil psicológico	Mensaje efectivo	Objetivo
Alto en Neuroticismo	"¡Peligro! Tu seguridad está en riesgo"	Generar miedo
Alto en Extraversión	"Únete a la fiesta del cambio"	Crear entusiasmo
Bajo en Amabilidad	"Ellos no merecen tu compasión"	Fomentar división
Alto en Apertura	"Nuevas ideas para un futuro mejor"	Promover innovación

Efectos de la microsegmentación (Cambridge Analytica; estimaciones ilustrativas del autor — la efectividad real de la empresa es discutida, ver Cap. 3): +20% en la intención de voto en grupos microsegmentados | -15% en la participación de votantes opuestos | 1,5 veces más efectiva que la publicidad tradicional. *Nota de rigor: la literatura experimental (PNAS 2024; MIT) encuentra que la ventaja persuasiva del microtargeting sobre estrategias alternativas es pequeña; el problema estructural que justifica la auditoría no es la eficacia persuasiva sino la asimetría de transparencia: la microsegmentación no auditable rompe la igualdad de armas electoral con independencia de su eficacia.*

Tecnologías de Perfilado Actuales (2026)

Tecnología	Datos recolectados	Precisión / Alcance
Análisis de redes sociales	Likes, compartidos, comentarios, tiempo de visualización	85-90% de precisión en preferencias políticas
Rastreo de navegación	Historial de búsqueda, cookies, tiempo en páginas	70% de los sitios web rastrea de alguna forma
Análisis de comportamiento	Patrones de compra, movimientos del ratón, pulsaciones	Optimización de mensajes en tiempo real
Biometría	Reconocimiento facial, voz, patrones de escritura	95% de precisión en identificación de emociones

Impacto de la Microsegmentación

Sobre la democracia: mensajes distintos para grupos distintos sobre el mismo tema (ejemplo Brexit: jóvenes urbanos → "el Brexit dañará tus oportunidades"; mayores rurales → "recuperará el control de las fronteras"; clase trabajadora → "los inmigrantes te quitan el trabajo"); división social; erosión de la verdad compartida.

Sobre la privacidad: recolección sin consentimiento informado, discriminación algorítmica, autonomía reducida por manipulación oculta.

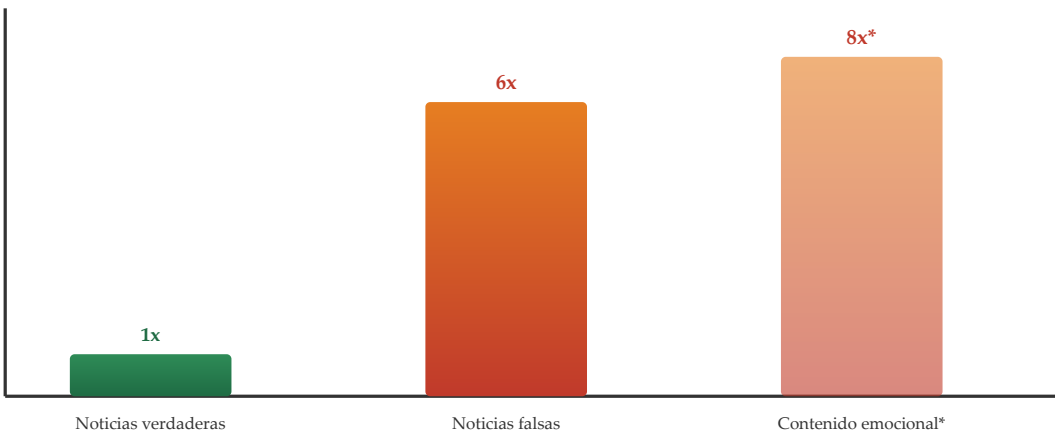
💡 **Datos preocupantes (2026):** 92% de los europeos no sabe que sus datos se usan para microsegmentación política | 78% se opondría si lo supiera | 65% de las campañas políticas usa microsegmentación | 40% del gasto en publicidad política va a microsegmentación. (Estimaciones ilustrativas del autor.)



Datos y Estadísticas del Capítulo

La Asimetría de la Viralidad: lo Falso Viaja Más Rápido

Velocidad de difusión relativa por tipo de contenido (noticias verdaderas = 1x)



= velocidad de las noticias verdaderas. Datos MIT/Science 2018 (Vosoughi, Roy, Aral): las falsas llegaron a 1.500 personas 6 veces más rápido y fueron un 70% más r

Figura 2.4 — Las noticias falsas se difunden seis veces más rápido que las verdaderas (cifra verificada). *Contenido emocional: estimación ilustrativa del autor.

*Estimación ilustrativa del autor para el contenido emocional; no es una cifra medida del estudio MIT. El estudio clave: los bots aceleraban verdades y falsedades por igual — la propagación la impulsan los humanos.

🔔 **La asimetría estructural que justifica este libro:** la noticia falsa promedio llega a **1.500 personas seis veces más rápido** que la verdadera y es un **70% más probable que se retuitee** (MIT/Science, 2018 — 126.000 historias, 3 millones de usuarios). La verdad empieza cada difusión con una desventaja estructural. Y el volumen se multiplica: los archivos deepfake en circulación crecieron de **~500.000 (2023) a ~8 millones (2025)**, mientras la detección humana se mantiene al borde del azar (**55,5%**). Ningún mecanismo de autorregulación del mercado corrige esta asimetría — solo una capacidad institucional permanente puede hacerlo (Parte II: EDSPA; Parte III: Poder Protector).

Comparación de Herramientas de Manipulación

Herramienta	Coste	Alcance	Detección	Impacto	Legalidad
Noticias falsas	Bajo	Alto	Media	Medio	Ilegal
Deepfakes	Alto → Bajo	Medio	Difícil	Alto	Ilegal
Burbujas de filtros	Bajo	Alto	Fácil	Alto	Legal
Microsegmentación	Alto	Alto	Difícil	Alto	Legal (regulada)
Bots	Bajo	Medio	Media	Medio	Ilegal



Fuentes y Referencias

Fuentes Académicas

1. Pariser, E. (2011). *The Filter Bubble*. Penguin Press.
2. Sunstein, C. R. (2017). *#Republic: Divided Democracy in the Age of Social Media*. Princeton University Press.
3. Zuboff, S. (2019). *The Age of Surveillance Capitalism*. PublicAffairs.
4. Tufekci, Z. (2018). *Twitter and Tear Gas*. Yale University Press.
5. Vosoughi, S., Roy, D., Aral, S. (2018). "The spread of true and false news online". *Science*, 359(6380).

Informes y Estudios

1. Comisión Europea (2018). *Informe sobre Desinformación: Una Amenaza para los Procesos Democráticos*.
2. Eurobarómetro (2025, 2026). *Actitudes hacia la Desinformación y las Redes Sociales*.
3. Oxford Internet Institute (2024). *Informe sobre Manipulación Computacional de la Opinión Pública*.
4. Sensity AI (2026). *Informe Anual sobre Deepfakes*.
5. AlgorithmWatch (2025). *Auditoría de Algoritmos de Recomendación*.
6. Washington University in St. Louis (2024). *Estudio experimental sobre engaño con deepfakes políticos (tasa de engaño 42%)*.
7. Meta-análisis de 56 estudios (2024). *Precisión humana de detección de deepfakes (55,54%)*.
8. iProov (2025). *Estudio de identificación de medios sintéticos (0,1% de acierto completo)*.

Casos de Estudio

1. BuzzFeed News (2017). Deepfake de Obama.
2. The New York Times (2022). Deepfake de Zelensky.
3. The Washington Post (2024). Robocall con voz de Biden en New Hampshire.
4. The Guardian (2018). Escándalo Cambridge Analytica.
5. SCMP/AFP (2024). Fraude Arup de Hong Kong (HK\$200M mediante videollamada deepfake).

Marcos Legales

1. Reglamento (UE) 2022/2065 — Ley de Servicios Digitales (DSA).
2. Reglamento (UE) 2024/1689 — Ley de IA de la UE.
3. Reglamento (UE) 2016/679 — Protección de datos (RGPD).

Conexión con el Resto del Libro

- **Capítulo 3:** La Vulnerabilidad Democrática → cómo estas herramientas afectan concretamente a la democracia
 - **Capítulo 4:** La Brecha de Soberanía → por qué Europa es particularmente vulnerable a estas amenazas
 - **Parte II (Capítulos 6-10 + 9B):** la EDSPA → la respuesta institucional temporal que detecta y contrarresta estas herramientas, y demuestra que la protección funciona
 - **Parte III (Capítulos 11-20):** el Poder Protector → la institucionalización permanente de la defensa frente al kit de manipulación
 - **Parte IV (Capítulo 21):** la visión final — el futuro no se predice: se construye
-

Capítulo 3: La Vulnerabilidad Democrática

Resumen del capítulo

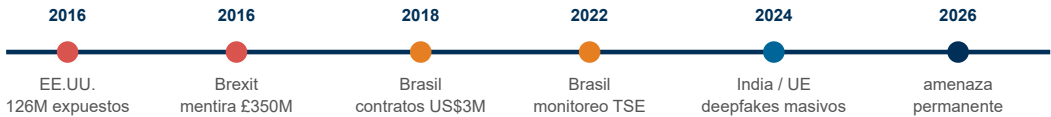
Este capítulo analiza cómo las herramientas descritas en el Capítulo 2 han operado contra sistemas democráticos concretos entre 2016 y 2026. Se examinan **cinco casos verificados de interferencia electoral** (Estados Unidos 2016, Brexit 2016, Brasil 2018-2022, India 2019-2024, Unión Europea 2019-2024), la polarización afectiva documentada por la literatura académica, la **paradoja de la confianza** —la confianza en la UE alcanza su máximo en 18 años mientras la confianza en lo nacional se erosiona— y la respuesta regulatoria europea (GDPR, DSA, AI Act). La conclusión es incómoda: la regulación ha llegado, pero no basta. Se necesita capacidad institucional permanente.

3.1 Estudios de caso: interferencia electoral (2016-2026)

Metodología de análisis: cada caso se examina según contexto, herramientas, actores, vectores, impacto medido y respuesta. Solo se presentan cifras verificables; las estimaciones van marcadas explícitamente.

Una década de interferencia documentada

Interferencia electoral documentada, 2016-2026



De campañas puntuales a una infraestructura de manipulación continua: el problema ya no es un episodio electoral, es el entorno informativo

Figura 3.1 — Cronología de la interferencia electoral. Elaboración propia sobre casos documentados.

Caso 1: Elecciones presidenciales de EE.UU. (2016)

La Agencia de Investigación de Internet (IRA) rusa operó una campaña de influencia a coste mínimo y alcance masivo. Facebook estimó ante el Senado que **126 millones** de estadounidenses pudieron ver contenido de la IRA entre 2015 y 2017, generado con solo **US\$100.000** en publicidad y unas 3.400 inserciones, frente a más de **61.500 publicaciones** orgánicas en Facebook y 116.000 en Instagram.

Métrica	Valor	Fuente
Alcance estimado en Facebook	126 millones de personas "alcanzadas"	Testimonio de Facebook al Senado (2017)
Inversión publicitaria IRA	~US\$100.000 en ~3.400 anuncios	Informe del Senado de EE.UU. (2018)
Publicaciones orgánicas	>61.500 en Facebook; 116.000 en Instagram	Informes New Knowledge / Senado
Compromiso en Instagram	187 millones de interacciones desde 133 cuentas	Informe del Senado (2018)
Lección estructural	US\$100.000 alcanzaron a un tercio de la población de una superpotencia: la asimetría es el dato central	

Nota de rigor: la cifra de 126 millones es la estimación de Facebook de personas que "pudieron ser alcanzadas" por al menos una historia de la IRA en dos años; parte de la literatura académica la considera maximalista y recuerda que solo el 11% del contenido de la IRA era explícitamente electoral. La magnitud es enorme incluso con la lectura más conservadora. Los estudios de exposición individual (p. ej., Guess, Nyhan y Tucker en *Nature Communications*) encuentran efectos actitudinales y de voto limitados; el daño documentado es ecosistémico: atacar cuesta casi cero, alcanzar a 126 millones cuesta US\$100.000, y ninguna democracia puede permitirse ese vector abierto.

Caso 2: Referéndum del Brexit (2016)

La campaña "Leave" combinó la **mentira del autobús** ("enviamos £350 millones semanales a la UE, financiamos el NHS en su lugar"), mensajería microsegmentada no auditable y amplificación automatizada. La Comisión Electoral británica multó a Leave.EU con **£70.000** por infracciones de financiación.

Nota de rigor: el papel de Cambridge Analytica en el Brexit es discutido: la empresa trabajó para la campaña, pero su propia efectividad fue puesta en duda por investigadores y periodistas. Este capítulo recoge el caso por lo verificable (mentira del autobús, mensajería segmentada, multa de la Comisión Electoral), no por las afirmaciones autopromocionales de la empresa.

- **Resultado:** 51,9% a favor de la salida; participación del 72,2%.
- **Efecto duradero:** la promesa del NHS sigue citándose años después como símbolo de desinformación rentable electoralmente — el "dividendo del mentiroso" en acción.
- **Lección:** la transparencia publicitaria llegó tarde (archivado de anuncios solo desde 2018); una mentira verificable que decide un referéndum irreversible.

Caso 3: Brasil (2018 y 2022)

2018: la investigación de *Folha de S.Paulo* reveló días antes de la segunda vuelta que empresarios conservadores habían firmado **contratos de hasta US\$3 millones** con agencias especializadas en mensajería masiva automatizada por WhatsApp a favor de Jair Bolsonaro — una práctica posiblemente constitutiva de **contribución ilegal de campaña**, que WhatsApp no podía auditar por su cifrado de extremo a extremo.

2022: ante la reelección de Lula (50,9%), el Tribunal Superior Electoral brasileño desplegó **monitoreo en tiempo real** y las plataformas limitaron los reenvíos masivos; pese a ello, las narrativas de fraude electoral penetraron lo suficiente para alimentar los asaltos institucionales del 8 de enero de 2023.

- **Lección 2018:** la mensajería cifrada es opaca incluso para la plataforma — el regulador llega tarde por diseño.
- **Lección 2022:** el monitoreo electoral en tiempo real funciona durante la jornada, pero no evita la deslegitimación posterior del resultado. La manipulación ya no termina con las urnas.

Caso 4: India (2019 y 2024)

Con **968 millones de electores** en 2024, India es el mayor experimento del mundo en democracia bajo IA generativa. La diferencia entre 2019 (desinformación masiva por WhatsApp) y 2024 es cualitativa: **deepfakes personalizados asequibles**, clonación de voz de líderes y contenido sintético a escala industrial. La respuesta incluyó la creación de la **Deepfakes Analysis Unit (DAU)** de la Misinformation Combat Alliance, un canal de WhatsApp para que los ciudadanos verificaran contenido.

- **Lección:** a escala india, ningún verificador de hechos humano alcanza; solo sistemas tecnológicos institucionales pueden procesar el volumen. Es el argumento de escala que sostiene la Parte II de este libro.

Caso 5: Unión Europea (2019 y 2024)

2019: la UE ya operaba con la East StratCom Task Force y EUvsDisinfo, pero con recursos minúsculos frente a la amenaza. **2024:** las elecciones al Parlamento Europeo se celebraron con el DSA en vigor, 200+ deepfakes documentados por la red EDMO, narrativas sobre migración y clima amplificadas y la participación en 51,2% (la segunda consecutiva por encima del 50%).

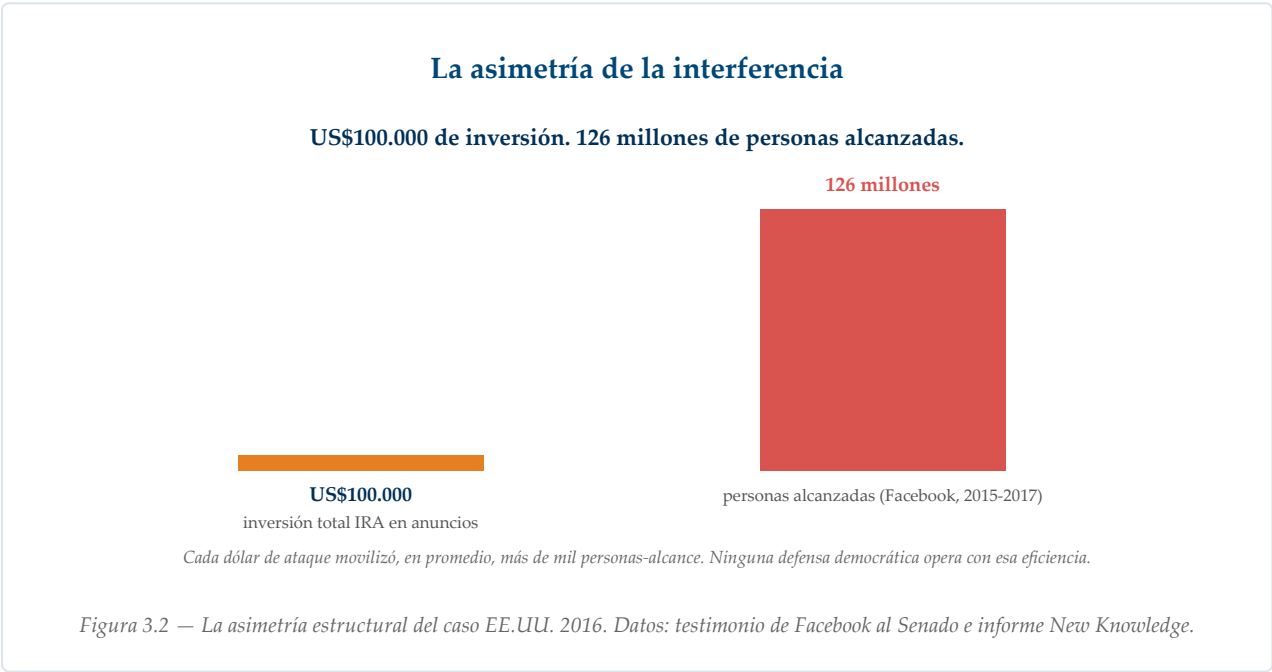
- **Avance:** por primera vez había obligaciones legales exigibles a las plataformas, no códigos voluntarios.
- **Límite:** la aplicación siguió siendo reactiva, nacional y fragmentada — el DSA sanciona conductas, pero no construye capacidad positiva de protección. Esa es exactamente la laguna que la EDSPA viene a cubrir.

3.2 Métricas de polarización social

Cómo se mide la polarización

- **Ideológica:** distancia entre posiciones medias de los electorados.
- **Afectiva:** sentimientos negativos hacia el votante del partido rival (termómetro 0-100). Es la más peligrosa: no se discrepa, se desprecia.
- **De elites:** hostilidad entre partidos y medios de referencia.

La evidencia académica más sólida sobre polarización afectiva en Europa procede del estudio de **Ansgar Reiljan (2020, European Journal of Political Research)**, que midió el "liking gap" entre votantes de partidos rivales en varios sistemas europeos. Sus hallazgos: los sistemas con mayor polarización afectiva en Europa son los del **sur y este del continente**, con España, Polonia y Hungría entre los más afectados, y la polarización afectiva puede ser alta incluso cuando la ideológica es moderada — es decir, *se puede odiar al rival sin que las posiciones políticas estén realmente lejos*. La manipulación explota exactamente esa brecha.



Burbujas y polarización en redes sociales

Nota metodológica: los porcentajes de usuarios "en burbujas" por plataforma no cuentan con series armonizadas verificables; la tabla siguiente es una **estimación ilustrativa del autor** construida sobre la literatura de exposición homogénea (Cap. 2) y debe leerse como orden de magnitud, no como medición.

Plataforma	% usuarios en burbujas (est.)*	Característica agravante
Twitter/X	~85%*	Diseño de confrontación pública
YouTube	~80%*	Bucle de recomendación de larga duración
Facebook	~78%*	83% de las noticias llegan por recomendación algorítmica (MIT, 2025)
Instagram	~72%*	Consumo pasivo de feed curado
TikTok	~68%*	Optimización por retención emocional pura
Patrón común	Ninguna plataforma optimiza para el encuentro entre posiciones distintas	

Consecuencias de la polarización

- **Parálisis democrática:** menos margen para compromisos; gobiernos en minoría y bloqueo institucional.
- **Deslegitimación cruzada:** el adversario no gana, "roba"; el resultado no se pierde, "se falsifica".
- **Mercado de la desinformación:** la polarización aumenta la demanda de contenido que humille al rival — es el combustible del ciclo del Cap. 2.

- **Violencia política:** la hostilidad afectiva es el mejor predictor verbal previo a incidentes violentos.

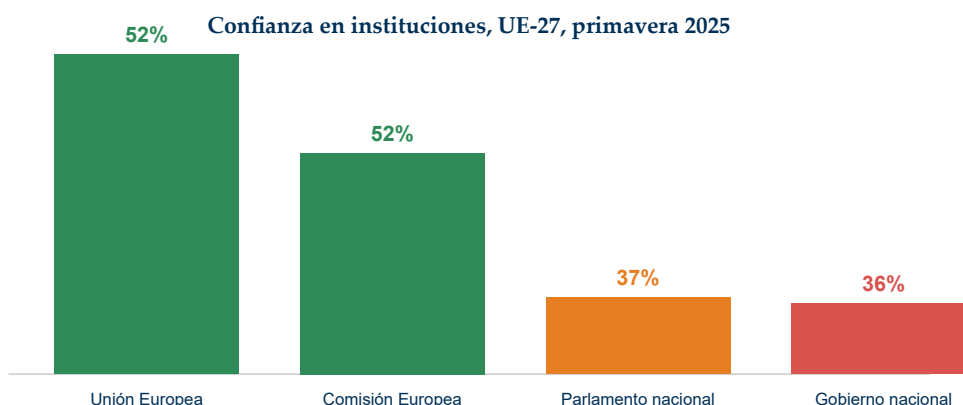
3.3 La paradoja de la confianza: Europa responde, lo nacional se erosiona

El hallazgo que reencuadra este capítulo —y que la V1 de este libro trataba de forma incorrecta al presentar una caída monótona de la confianza— surge del **Eurobarómetro Estándar 103 (primavera 2025)**:

La confianza en la Unión Europea alcanzó en 2025 su nivel más alto en 18 años: el 52% de los europeos confía en la UE y en la Comisión Europea, frente al 31% de 2013. Pero solo el 36% confía en su gobierno nacional y el 37% en su parlamento nacional.

— Eurobarómetro Estándar 103, primavera 2025

La paradoja de la confianza (2025)



Verde: confianza en máximos de 18 años. Rojo/naranja: erosión nacional. Fuente: Eurobarómetro Estándar 103 (2025).

Figura 3.3 — La paradoja de la confianza. Los ciudadanos castigan a lo nacional y refuerzan a lo europeo.

Por qué es una paradoja informativa

La desinformación no erosiona uniformemente: golpea donde la narrativa nacional tiene más superficie de ataque —gobiernos, partidos, medios nacionales— mientras la UE, más lejana del ruido mediático cotidiano y asociada a respuestas visibles (vacunas, recuperación post-COVID, apoyo a Ucrania), **sube**. El dato decisivo para este libro: entre los jóvenes de 15 a 24 años la confianza en la UE alcanza el **59%**, y el 75% de los europeos se siente ciudadano de la UE, el nivel más alto en más de dos décadas.

El argumento que funda el libro

Si la confianza en la UE está en su máximo de 18 años precisamente cuando la confianza en lo nacional se erosiona, entonces la capacidad de protección cognitiva **debe ser europea**: los ciudadanos ya están diciendo en qué nivel confían para protegerlos. La paradoja de la confianza no es una curiosidad estadística; es el mandato implícito de la opinión pública europea para una EDSPA. La Parte II (capítulos 6-10 y 9B) responde a ese mandato; la Parte III (capítulos 11-20) le da rango constitucional.

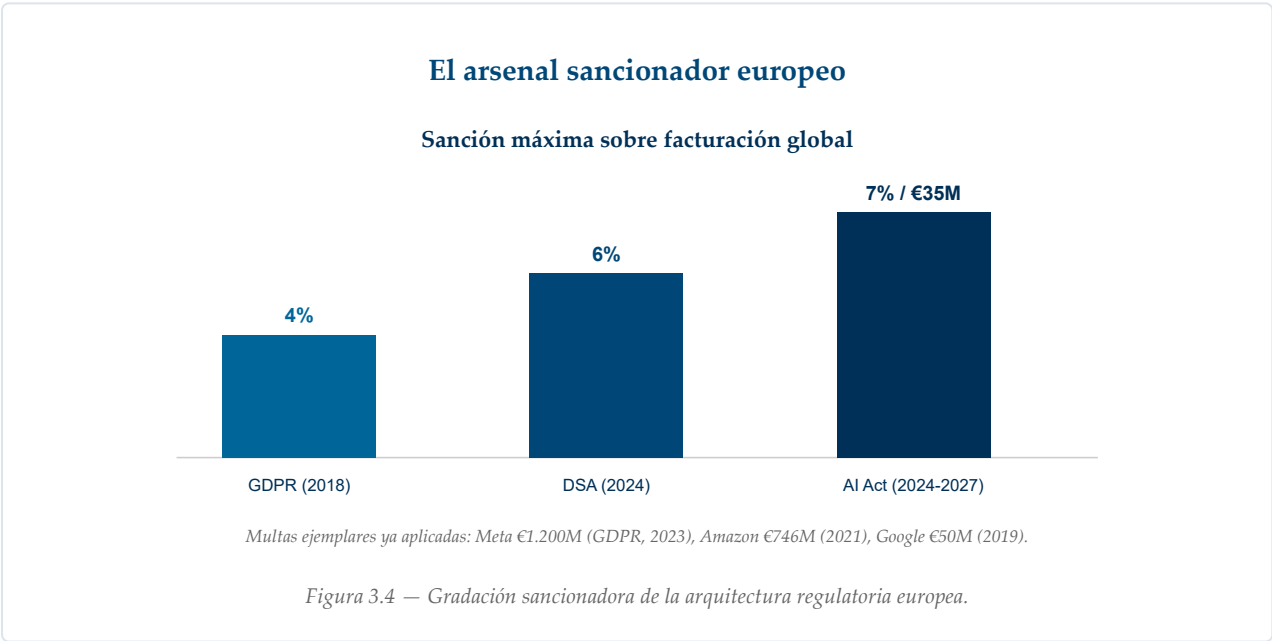
Donde la erosión sí es real

La erosión concentrada se observa en partidos políticos (sistemáticamente la institución menos fiable en toda Europa), en medios tradicionales —cada vez más atrapados en la acusación cruzada de sesgo— y en el proceso electoral, cuando la deslegitimación post-votación se instala, como demostraron EE.UU. 2020 y Brasil 2022.

3.4 La respuesta regulatoria de la UE: necesaria, insuficiente

Entre 2018 y 2024 la UE construyó el marco regulatorio digital más avanzado del mundo. Es un éxito real — y también la prueba de que la regulación sola no protege.

Instrumento	Año	Qué hace	Sanción máxima	Límite estructural
GDPR	2018	Control de datos personales; frena la microsegmentación salvaje	4% facturación global	No aborda la desinformación
Código de Prácticas sobre Desinformación	2018/2022	Autorregulación con verificación de cumplimiento	Ninguna (es voluntario)	Sin dientes jurídicos
EDMO	2020	Red europea de verificación y monitoreo de narrativas	N/A	Coordina, no protege directamente
DSA	2022/2024	Transparencia algorítmica, evaluaciones de riesgo, deberes para VLOPs (plataformas de más de 45 millones de usuarios en la UE)	6% facturación global	Reactiva: sanciona conductas ya producidas
AI Act	2024	Prohíbe manipulación subliminal; etiquetado obligatorio de deepfakes	7% facturación global o €35M	Aplicación gradual hasta 2027
Balance conjunto	Reglas sin capacidad operativa propia: Europa puede multar a las plataformas, pero no puede detectar, rastrear y desactivar campañas de manipulación en tiempo real			



Efectividad verificada

- **Logros:** transparencia publicitaria real, evaluaciones de riesgo obligatorias para VLOPs, primer marco del mundo que obliga a etiquetar deepfakes (AI Act), coordinación de verificadores vía EDMO.
- **Limitaciones:** aplicación desigual entre Estados, tecnología que evoluciona más rápido que la norma, plataformas renuentes a compartir datos, y —la más importante— **nadie en Europa tiene el trabajo de proteger activamente la esfera cognitiva:** todos vigilan conductas pasadas, nadie construye defensa presente.

La laguna que justifica la Parte II

El DSA castiga a quien ya manipuló. El AI Act etiqueta el deepfake que ya circula. El GDPR protege los datos ya recolectados. Falta la pieza que el Capítulo 6 presentará: una **agencia europea con capacidad operativa permanente** —detección temprana, rastreo de campañas coordinadas, respuesta en tiempo real, resiliencia estructural—. La regulación es el esqueleto jurídico; la EDSPA es el sistema inmunológico que este diagnóstico demuestra imprescindible.

Datos y estadísticas del capítulo

Síntesis numérica verificada

Dato	Valor	Fuente
Personas alcanzadas por la IRA (EE.UU., 2015-2017)	126 millones (estimación Facebook)	Testimonio al Senado / informes 2018
Inversión IRA en anuncios	~US\$100.000	Informe del Senado (2018)
Multa a Leave.EU	£70.000	Comisión Electoral del Reino Unido
Contratos de mensajería masiva (Brasil 2018)	hasta US\$3 millones por contratante	Folha de S.Paulo (2018)
Confianza en la UE / Comisión (2025)	52% / 52% — máximo en 18 años	Eurobarómetro Estándar 103
Confianza en gobierno / parlamento nacionales	36% / 37%	Eurobarómetro Estándar 103
Jóvenes 15-24 que confían en la UE	59%	Eurobarómetro Estándar 103
Sanciones máximas GDPR / DSA / AI Act	4% / 6% / 7% facturación global	Reglamentos UE

Fuentes

- Informe del Senado de EE.UU. / New Knowledge (2018). *The Tactics & Tropes of the Internet Research Agency*.
- Testimonios de Facebook, Twitter y Google ante el Senado de EE.UU. (2017-2018).
- Folha de S.Paulo (octubre 2018). Investigación sobre contratos de mensajería masiva por WhatsApp.
- The Conversation / PBS (2018). *WhatsApp skewed Brazilian election*.
- Comisión Electoral del Reino Unido (2018). Informe sobre el referéndum de 2016.
- Reiljan, A. (2020). "Fear and loathing across party lines (also) in Europe: Affective polarisation in European party systems". *European Journal of Political Research*, 59(2).
- Eurobarómetro Estándar 103 (primavera 2025). Confianza en las instituciones.
- Comisión Europea (2022-2025). Aplicación del DSA e informes del Código de Prácticas sobre Desinformación.
- EDMO (2024). Monitoreo de las elecciones al Parlamento Europeo.
- Misinformation Combat Alliance / WEF (2024). Lecciones de la Deepfakes Analysis Unit india.

Conexión con el resto del libro

Este capítulo ha demostrado que la vulnerabilidad democrática es real, medible y creciente, y que la regulación —necesaria— es insuficiente. El **Capítulo 4** (La Brecha de Soberanía) explica por qué Europa no puede depender de otros para su protección cognitiva; el **Capítulo 5** cuantifica el coste de la inacción. La **Parte II** (capítulos 6-10 y 9B) diseña la respuesta institucional: la EDSPA. La **Parte III** (capítulos 11-20) la eleva a cuarto poder constitucional de Europa.

Capítulo 4: La Brecha de Soberanía

Resumen del capítulo

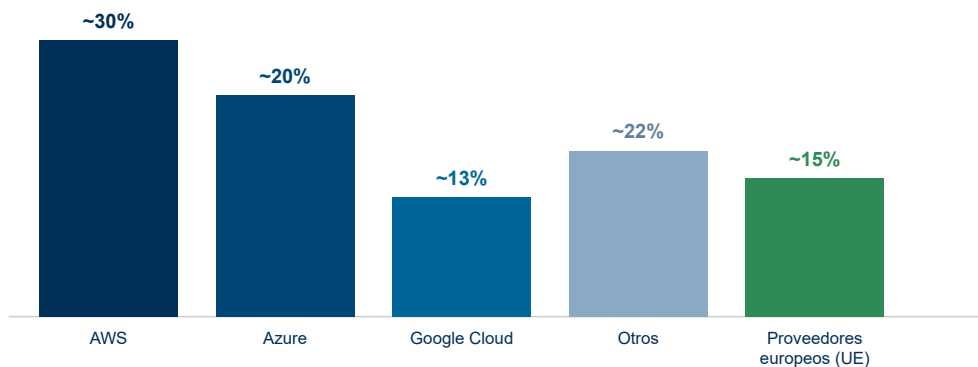
Europa protege su esfera cognitiva con infraestructura que no controla. Los tres hyperscalers estadounidenses controlan en torno a **dos tercios del mercado mundial de nube** (Synergy Research, Q3 2025) y los proveedores europeos apenas el **~15% de su propio mercado**; los modelos de IA frontera que usan empresas e investigadores europeos son en su inmensa mayoría estadounidenses; y en **junio de 2026** Estados Unidos demostró que ese control es un instrumento de política exterior: una Orden Ejecutiva sobre IA avanzada y una directiva de control de exportaciones notificada a Anthropic que exige licencia para transferir sus modelos Mythos y Fable incluso a personas extranjeras dentro de EE.UU. Este capítulo cuantifica esa brecha de soberanía —infraestructura, datos, modelos, talento— y concluye que sin capacidad tecnológica propia, la protección cognitiva europea es una prerrogativa prestada.

4.1 Dependencia tecnológica de potencias extranjeras

Definición: situación en la que una región depende de tecnología desarrollada, controlada o alojada en el extranjero para funciones críticas de su sociedad, su economía y su gobierno. La dependencia no es un problema de eficiencia: es un problema de *voluntad ajena*.

El mapa real de la dependencia (2026)

Mercado mundial de infraestructura de nube (2026)



AWS, Azure y Google Cloud: ~63% mundial (Synergy Research, Q3 2025). Europeos: ~15% del propio mercado europeo. Fuente: Synergy / Holori 2025.

Figura 4.1 ➤ Dominación de los tres hyperscalers de EE.UU. (~63% mundial, ~15% europeo): una dependencia estructural de la infraestructura extranjera.

Las cuatro capas de la dependencia

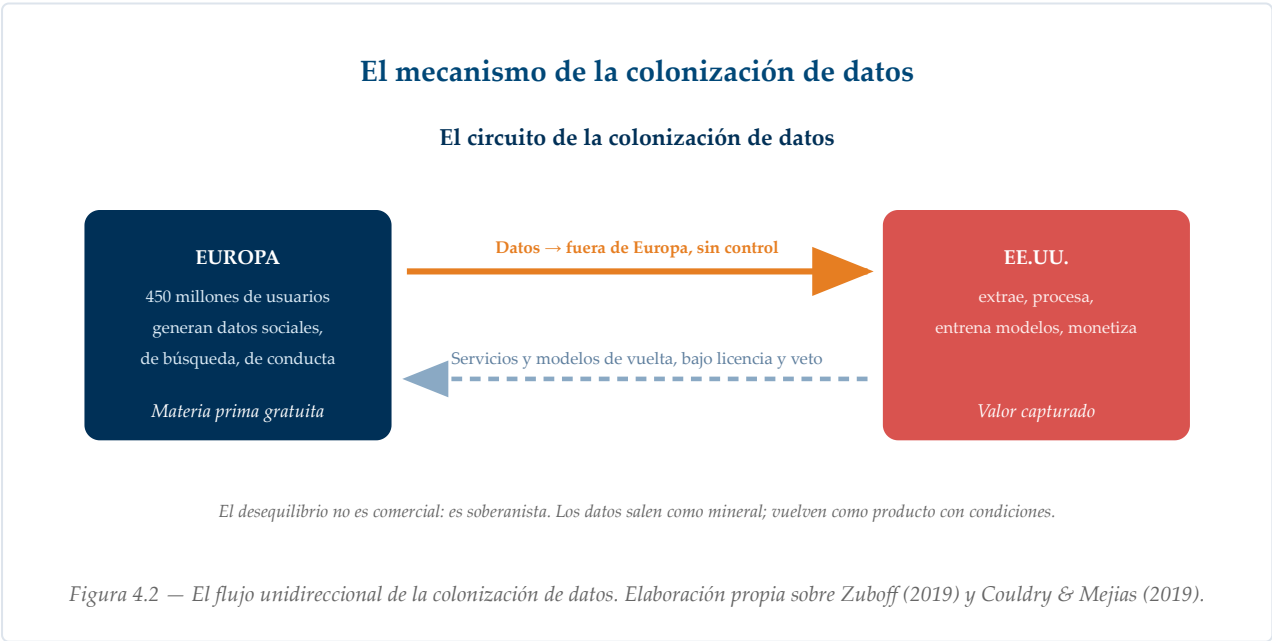
Capa	Situación verificada (2026)	Actores europeos
Infraestructura de nube	Los tres hyperscalers de EE.UU. controlan ~63% mundial; los europeos ~15% de su propio mercado	OVHcloud, T-Systems, STACKIT, Hetzner, Scaleway
Modelos de IA frontera	Uso europeo dominado por modelos de EE.UU.* (estimación ilustrativa del autor: ~90-95%*)	Mistral AI (valorada en ~€11.700M), Cohere-Aleph Alpha, Black Forest Labs, DeepL, Kyutai, AMD Silo AI
Sistemas operativos	Windows, macOS, Android, iOS (todos de EE.UU.) cubren prácticamente el mercado europeo*	Sin alternativa a gran escala
Acceso a datos de plataformas	Depende de APIs de empresas de EE.UU., recortadas unilateralmente (sección 4.4)	Sustitución parcial vía DSA art. 40 (investigadores vetted)
Consecuencia	Cada capa de la protección cognitiva potencial de Europa pasa por una decisión empresarial o regulatoria estadounidense	

El precedente jurídico: la ley CLOUD (2018)

La **CLOUD Act** estadounidense de 2018 permite a las autoridades de EE.UU. exigir a empresas estadounidenses datos alojados **en cualquier lugar del mundo**. Combinada con el fallo **Schrems II** del Tribunal de Justicia de la UE (2020), que invalidó el Privacy Shield precisamente por el riesgo de acceso estadounidense a datos europeos, la consecuencia es directa: los datos de ciudadanos europeos en nubes estadounidenses están bajo jurisdicción de un tercer Estado. La infraestructura de detección de desinformación europea, si se construye sobre nube estadounidense, arrastra esa vulnerabilidad por diseño.

4.2 Colonización de datos: el flujo unidireccional

El concepto procede de la crítica académica del capitalismo de la vigilancia: **Shoshana Zuboff** (*La era del capitalismo de la vigilancia*, 2019) describió la extracción y monetización de la experiencia humana como materia prima; **Nick Couldry y Ulises Mejias** (2019) lo nombraron directamente: "colonización de datos", el proceso por el cual los datos de personas de otras regiones se extraen, procesan y monetizan sin beneficio proporcional para sus comunidades.



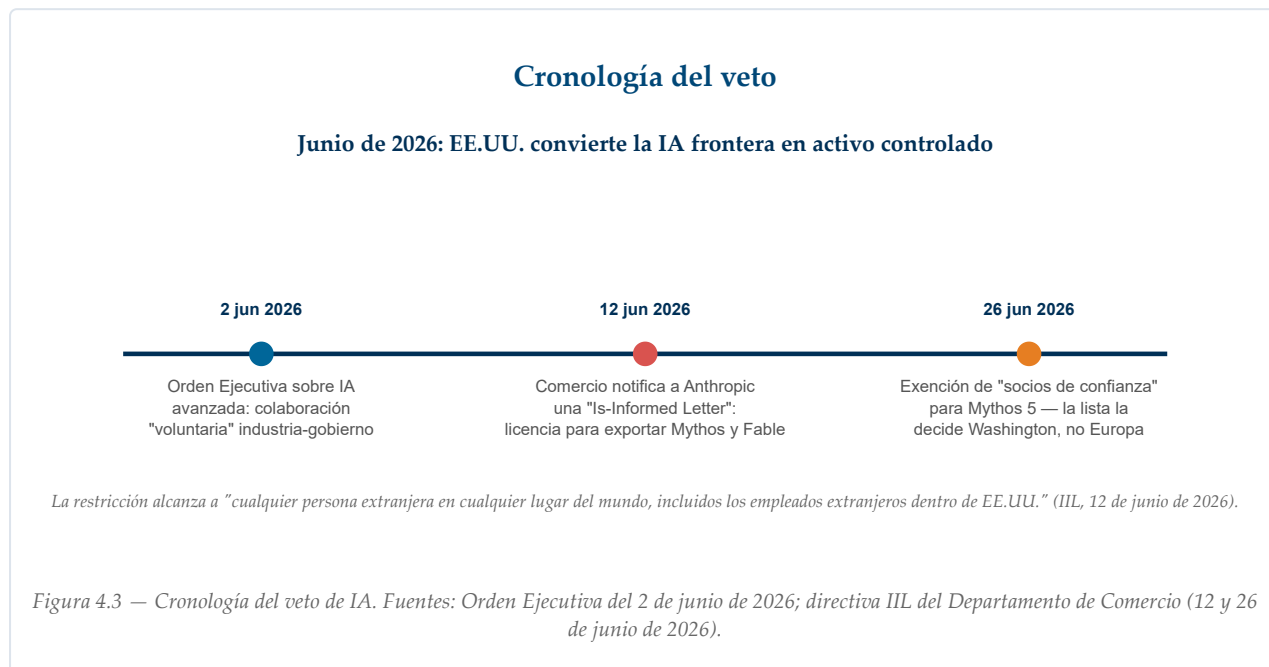
El tamaño real de la economía de datos europea

Las cifras verificadas del **European Data Market Monitoring Tool** (Comisión Europea, 2025) dimensionan lo que está en juego: el mercado de datos de la UE27 creció de **€82.000M (2023) a €90.000M (2024)**, y la economía de datos superará **€630.000M en 2025 (~4,7% del PIB)**, camino de €815.000M en 2030. El informe Draghi (2024) subraya

la contradicción: ese valor se genera sobre datos europeos, pero se captura mayoritariamente en plataformas no europeas.

4.3 El veto de IA de EE.UU. (junio de 2026)

Lo que este capítulo anticipaba como hipótesis ocurrió en junio de 2026, y con nombres propios. La secuencia verificada:



Qué significa para la protección cognitiva

- **Un precedente, no un caso único:** la arquitectura del control ya existe; aplicarla a otros modelos es una decisión administrativa, no una ley nueva.
- **La detección de desinformación es IA frontera:** los mejores sistemas de detección de deepfakes y campañas coordinadas se entrenan con la misma clase de modelos que ahora están sujetos a licencia. Europa no puede basar su defensa cognitiva en herramientas cuya disponibilidad depende de un permiso de Comercio de EE.UU.
- **"Socios de confianza" es una jerarquía, no una alianza:** la exención del 26 de junio la concede Washington caso por caso. La soberanía no se delega; se ejerce o no existe.
- **El precedente semiconductor:** es el mismo mecanismo ya aplicado a China en chips — ahora extendido a la IA y a los aliados.

El argumento decisivo de este capítulo

El veto de junio de 2026 demostró que la capacidad de IA es un **activo estratégico bajo control estatal**, disponible para los socios como privilegio revocable. *Nota de rigor: no es un gesto de una sola administración — la primera regla de difusión (Biden, enero de 2025) fue retirada en mayo de 2025; la segunda (Trump, EO 14409 e IIL de junio de 2026) lleva vigente desde entonces: dos administraciones, dos instrumentos distintos, la misma palanca. El patrón bipartidista es el dato estructural.* Una Europa que quiera proteger su esfera cognitiva necesita soberanía de cómputo: modelos propios, nube propia y datos propios. La EDSPA de la Parte II (capítulos 6-10 y 9B) se diseña sobre ese triángulo; el Poder Protector de la Parte III (capítulos 11-20) le añade la garantía constitucional.

4.4 Restricciones de acceso a datos: la opacidad como política de facto

El cierre de CrowdTangle (2024)

El 14 de agosto de 2024 Meta cerró CrowdTangle, la herramienta que permitía a periodistas e investigadores rastrear desinformación en Facebook e Instagram. Su sustituto, Meta Content Library, es **menos transparente y accesible**: menos funciones en los once temas clave auditados, proceso de acceso lento y restrictivo, sin capacidad de seguimiento del rendimiento de listas personalizadas — justo en el año de más de sesenta elecciones mundiales (investigación conjunta de Proof News, Tow Center y Algorithmic Transparency Institute, 2024).

El patrón se repite

Plataforma	Restricción	Consecuencia para la protección cognitiva
Meta	CrowdTangle cerrado (ago 2024); acceso a Content Library selectivo y lento	Ceguera parcial para rastrear desinformación en Facebook/Instagram
X (Twitter)	API cerrada a precios prohibitivos desde 2023	Herramientas de detección de bots y redes coordinadas degradadas
TikTok	Acceso a datos mínimo para investigadores	La plataforma preferida por los jóvenes es prácticamente inauditable
Patrón	La transparencia que las plataformas concedieron bajo presión (2016-2020) se ha retirado en cuanto la presión bajó. El acceso a datos no es un derecho: es una concesión revocable.	

La respuesta europea: DSA artículo 40

Por primera vez, el **artículo 40 del DSA** obliga a las plataformas muy grandes a dar acceso a datos a investigadores acreditados ("vetted researchers") designados por centros de competencia digitales. Es un avance real — y también una demostración de lentitud: los primeros accesos llegaron años después de la entrada en vigor, con litigios de por medio. La regulación obliga a compartir; no construye capacidad propia de análisis. Esa es la diferencia entre transparencia concedida y soberanía ejercida.

4.5 La necesidad de soberanía digital europea

Definición: la capacidad de una región para controlar su propio destino digital —infraestructura, datos, tecnologías y normas—. La soberanía cognitiva es su capa superior: sin infraestructura propia no hay detección propia; sin detección propia no hay protección posible.

Europa ya tiene activos: supercomputación (EuroHPC)

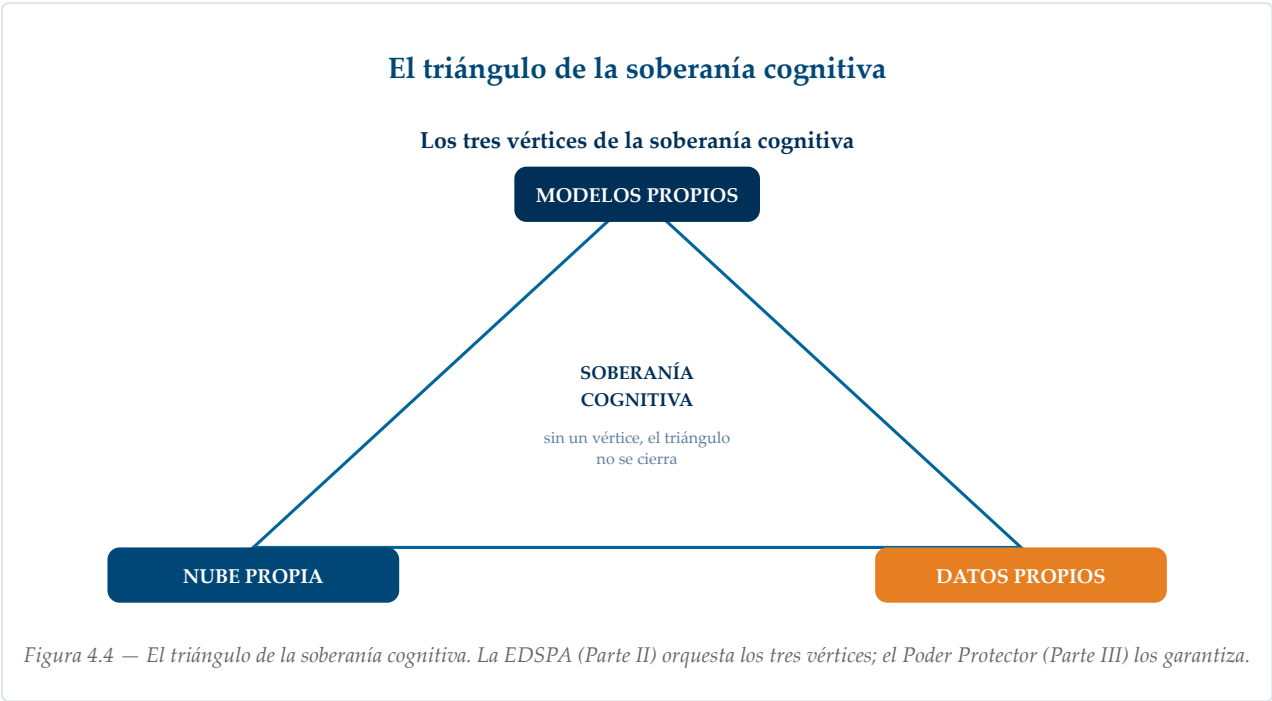
La Joint Undertaking EuroHPC financia **doce superordenadores de última generación** repartidos por Europa. Es la prueba de que cuando Europa decide construir capacidad, lo hace — y es la base de cómputo sobre la que entrenar modelos soberanos.

Superordenador	País	Potencia	Año
JUPITER	Alemania (Jülich)	~1 exaFLOP — primer exaescala de Europa	2025
LUMI	Finlandia (Kajaani)	~386 petaFLOPS	2022
Leonardo	Italia (Bologna)	~249 petaFLOPS	2022
MareNostrum 5	España (Barcelona)	~215 petaFLOPS	2023
MeluXina	Luxemburgo	~13 petaFLOPS	2022
Red EuroHPC	12 superordenadores	Base de cómputo soberana para IA europea y detección a escala	

El triángulo de la soberanía cognitiva

- **Modelos propios:** Mistral AI (Francia, valorada ~€11.700M), Cohere-Aleph Alpha (Alemania), Black Forest Labs, DeepL, Kyutai, AMD Silo AI — la vanguardia europea existe; necesita demanda pública estable para escalar.

- **Nube propia:** OVHcloud, T-Systems, STACKIT, Hetzner — con el impulso del marketplace soberano (Gaia-X / IPCEI-CIS) para que el sector público europeo compre europeo.
- **Datos propios:** espacios de datos comunes europeos (salud, movilidad, energía) con €2.000M del programa Digital Europe.



La lección del capítulo

La brecha de soberanía no es una lamentación: es un inventario de lo que falta. Cada pieza —modelos, nube, datos, acceso a plataformas— ya tiene un embrión europeo verificable. Lo que falta es la **institución que los orqueste con una misión de protección**. El Capítulo 5 cierra el diagnóstico cuantificando el coste de no tenerla; la Parte II (capítulos 6-10 y 9B) presenta la EDSPA como esa orquestación; la Parte III (capítulos 11-20) la eleva a Poder Protector constitucional.

Datos y estadísticas del capítulo

Dato	Valor	Fuente
Cuota mundial de nube de los 3 hyperscalers de EE.UU.	~63% (AWS ~30%, Azure ~20%, Google ~13%)	Synergy Research (2026)
Cuota de proveedores europeos en el mercado europeo	~15%	Holori / análisis de mercado 2026
Mercado de datos UE27	€82.000M (2023) → €90.000M (2024)	European Data Market Monitoring Tool (2025)
Economía de datos UE27	>€630.000M en 2025 (~4,7% del PIB); €815.000M previstos en 2030	EDM Monitoring Tool / Draghi (2024)
Valoración de Mistral AI	~€11.700M (ronda de sept. 2025)	Informes de financiación 2025-2026
Cierre de CrowdTangle	14 de agosto de 2024	Meta Transparency Center / CJR
IIL a Anthropic (Mythos y Fable)	12 de junio de 2026; exención "trusted partners" 26 de junio	Departamento de Comercio de EE.UU. (2026)
Superordenadores EuroHPC	12, incluido JUPITER (~1 exaFLOP, el 1º de Europa)	EuroHPC JU (2026)

Fuentes

- Synergy Research Group (2026). Tracker trimestral de infraestructura de nube, Q1 2026.
- Holori (2026). *Cloud Market Share 2026*; análisis de mercado europeo.
- Comisión Europea (2025). *European Data Market Monitoring Tool — First Report on Facts and Figures*.
- Draghi, M. (2024). *The Future of European Competitiveness*.
- Orden Ejecutiva de EE.UU. sobre IA avanzada (2 de junio de 2026) y directivas IIL del Departamento de Comercio (12 y 26 de junio de 2026), documentadas por Mayer Brown (2026).
- Zuboff, S. (2019). *The Age of Surveillance Capitalism*. PublicAffairs.
- Couldry, N. y Mejias, U. (2019). *The Costs of Connection*. Stanford University Press.
- CJR / Proof News / Tow Center / Algorithmic Transparency Institute (2024). Auditoría del cierre de CrowdTangle y de Meta Content Library.
- EuroHPC Joint Undertaking (2026). Catálogo de superordenadores.
- Tribunal de Justicia de la UE (2020). Sentencia Schrems II (C-311/18); CLOUD Act de EE.UU. (2018).

Conexión con el resto del libro

La Parte I ha completado el diagnóstico: la amenaza (Cap. 1-3) y ahora la imposibilidad de defenderse con herramientas prestadas. El **Capítulo 5** cuantifica el coste de la inacción y cierra la Parte I. La **Parte II** (capítulos 6-10 y 9B) diseña la EDSPA —la agencia que convierte la soberanía de cómputo en protección cognitiva operativa— y la **Parte III** (capítulos 11-20) la institucionaliza como el cuarto poder de Europa.

Capítulo 5: La Urgencia de la Protección

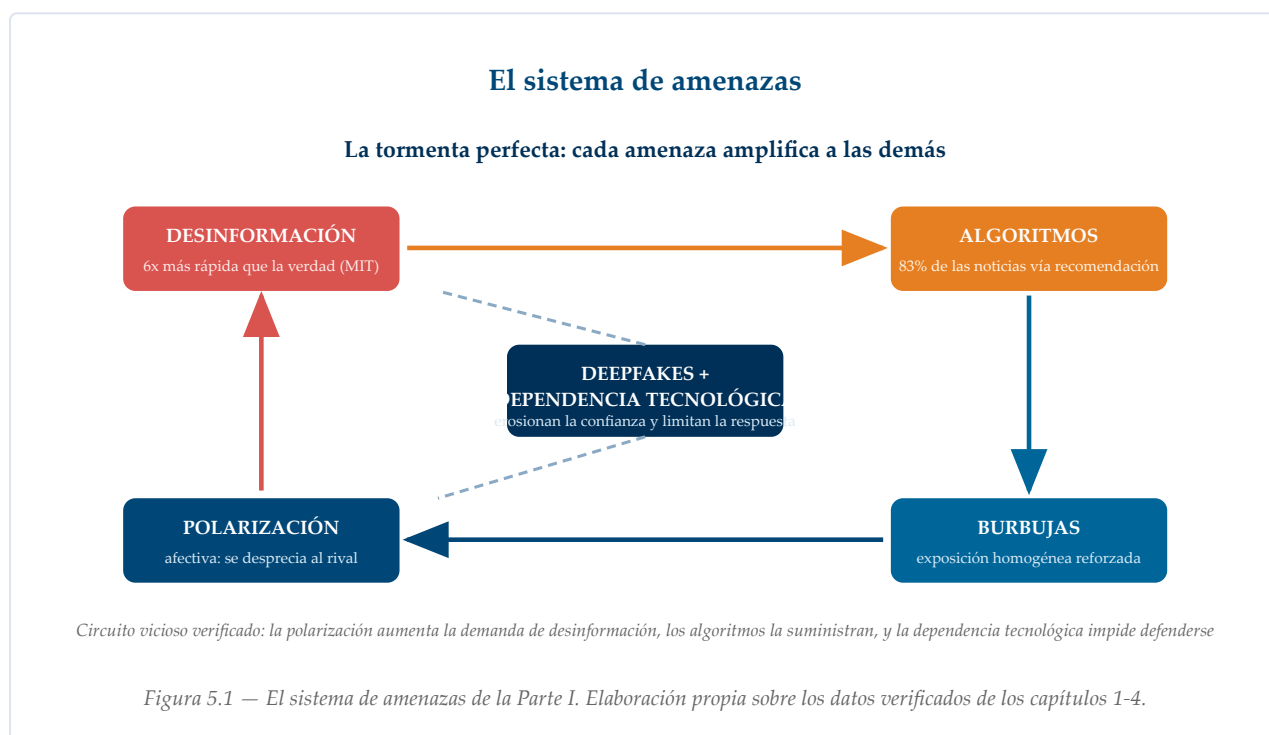
Síntesis del diagnóstico: las amenazas se refuerzan entre sí, los mecanismos actuales están fragmentados y subfinanciados, y cada año sin capacidad propia tiene un coste medible

Resumen del capítulo

Este capítulo cierra la Parte I. Sintetiza las amenazas verificadas de los capítulos 1-4, inventaría los mecanismos de protección existentes con sus **presupuestos reales** —y la comparación es elocuente: la unidad central de EDMO opera con **€2,5 millones** y East StratCom con unos **€11 millones y 40 expertos**, frente a Frontex con **~€1.100 millones anuales** para la frontera física—, analiza los cuellos de botella institucionales de la UE y argumenta el caso para una protección dedicada: la EDSPA, con la cooperación reforzada como vía de arranque. La conclusión: ninguna institución europea tiene hoy, como misión central, proteger la esfera cognitiva de los europeos.

5.1 Síntesis de las amenazas: la tormenta perfecta

Los capítulos 1-4 no describieron cuatro problemas distintos, sino **un sistema de amenazas interdependiente**. Cada componente amplifica a los demás:

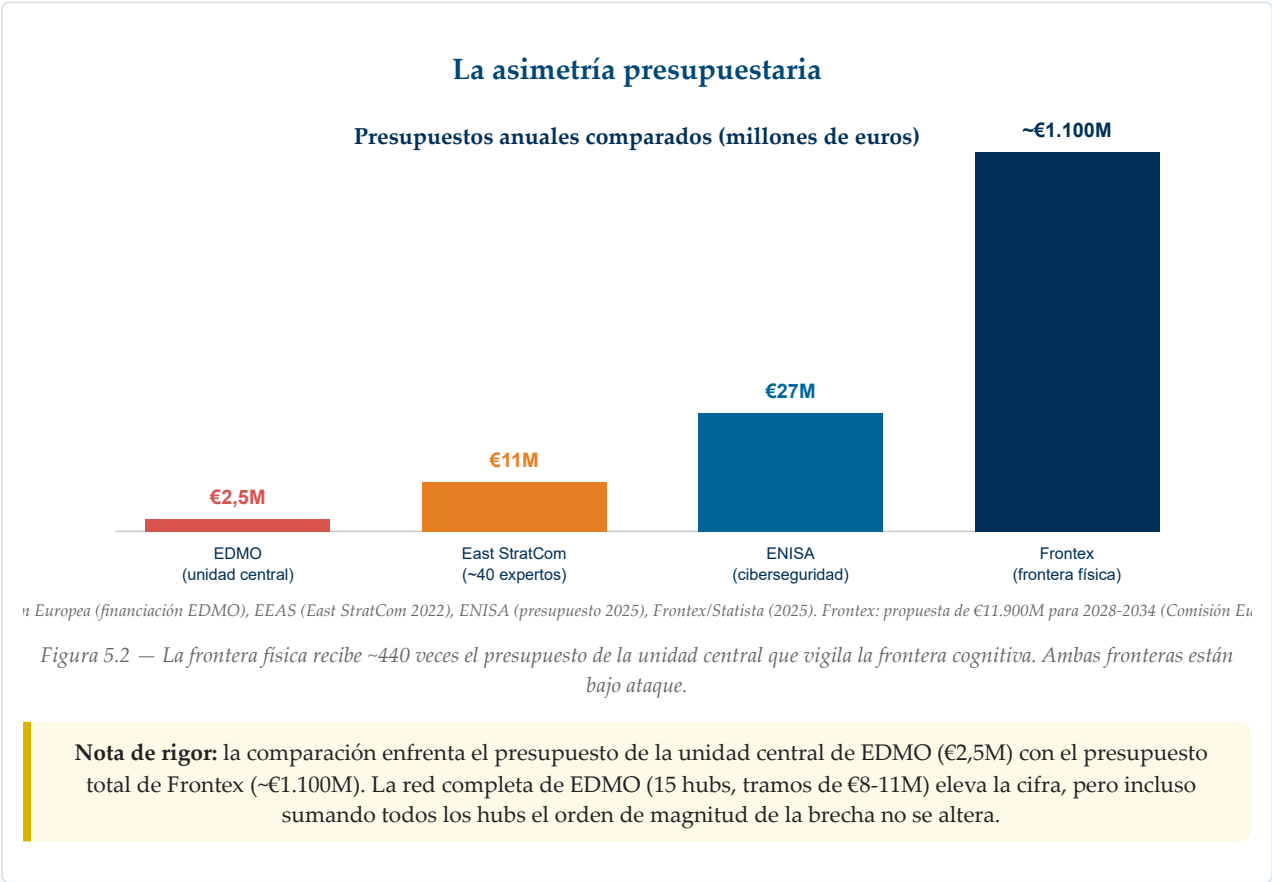


El diagnóstico en cifras verificadas

Capítulo	Hallazgo clave	Cifra verificada	Fuente
Cap. 1	La esfera cognitiva es el nuevo campo de batalla	116.175 despidos atribuidos a IA en EE.UU. (ene-ago 2026)	Reportes de empleo 2026 / Cap. 5 del libro
Cap. 2	La falsedad se propaga más rápido que la verdad	6x más rápido; 70% más retweets	Vosoughi et al., <i>Science</i> 2018 (MIT)
Cap. 2	Los humanos no detectan deepfakes	55,5% de acierto; 0,1% los identifica todos	Meta-análisis 56 estudios 2024 / iProov 2025
Cap. 3	La interferencia es barata y masiva	US\$100.000 alcanzaron a 126 millones (EE.UU. 2016)	Testimonio de Facebook al Senado
Cap. 3	La confianza se erosiona en lo nacional, no en lo europeo	UE 52% (máximo 18 años) vs gobierno nacional 36%	Eurobarómetro 103 (2025)
Cap. 4	La IA frontera es un activo controlado por EE.UU.	IIL a Anthropic (Mythos/Fable), junio 2026	Dept. de Comercio de EE.UU.
Cap. 4	La infraestructura de defensa no es europea	~63% de nube mundial en 3 hyperscalers de EE.UU.; ~15% europea en Europa	Synergy Research Q3 2025
Balance	Amenaza transnacional, operativa y barata. Defensa nacional, fragmentada y carísima.		

5.2 Los mecanismos actuales y sus presupuestos reales

Europa no está desarmada: tiene regulación avanzada (Cap. 3) e instituciones de monitoreo. Lo que no tiene es **escala**. La comparación presupuestaria verificada lo muestra sin piedad:



Inventario de mecanismos y límites

Mecanismo	Función	Recursos verificados	Límite estructural
EDMO (2020)	Red de verificación: 15 hubs en toda la UE, academia + verificadores	Central: €2,5M; hubs en tramos de €8-11M	Coordina y observa; sin capacidad operativa ni potestad de actuación
East StratCom / EUvsDisinfo (2015)	Monitoreo de desinformación prorrusa; base de datos con miles de casos	~€11M y ~40 expertos (2022)	Foco exclusivo en el vector ruso; sin mandato sobre manipulación doméstica o comercial
ENISA (2004)	Agencia de ciberseguridad de la UE	€26,9M anuales (2025) + €36M Reserva Ciber	Ciberseguridad ≠ protección cognitiva: no aborda desinformación ni manipulación
Viginum (Francia, 2021)	Vigilancia de interferencias extranjeras en línea	Escala nacional	Solo Francia; una agencia europea no puede apoyarse en capacidades de un solo Estado
Hueco común	Ninguna institución tiene detección temprana + investigación + respuesta en tiempo real como misión central, a escala europea		

Las siete limitaciones estructurales

- **Fragmentación:** EDMO, East StratCom, ENISA, agencias nacionales y unidades electorales trabajan en paralelo, sin centro de mando.
- **Subfinanciación:** decenas de millones contra una industria de la manipulación que opera a escala de plataformas de miles de millones de usuarios.
- **Reacción, no prevención:** los desmentidos llegan cuando la desinformación ya cumplió su ciclo — que es 6 veces más rápido que la verdad (Cap. 2).
- **Dependencia de plataformas:** los datos para detectar campañas son una concesión revocable de empresas de EE.UU. (Cap. 4).
- **Falta de especialización:** la protección cognitiva requiere perfiles que hoy no existen en ningún organigrama europeo: analistas de campañas coordinadas, ingenieros de detección de deepfakes, juristas de libertad de expresión trabajando juntos.
- **Fronteras digitales vs respuestas nacionales:** una campaña nace en un país, se amplifica desde otro y golpea al tercero; las competencias se detienen en cada frontera.
- **Ritmo tecnológico:** el DSA se diseñó antes de la IA generativa; el AI Act se aplicará gradualmente hasta 2027. La ley siempre llega después de la herramienta.

5.3 Los cuellos de botella institucionales

Supongamos que mañana la UE decidiera crear la capacidad que falta. ¿Cuánto tardaría? Los precedentes verificados:

Instrumento	De la propuesta a la aplicación	Lección
DSA	Propuesta dic. 2020 → aplicación plena 2024: ~4 años	El ritmo regulatorio más rápido posible en un tema « caliente »
AI Act	Propuesta abr. 2021 → aprobación 2024 → aplicación gradual hasta 2027: ~6 años	La aplicación por fases añade años a los años
Implicación	Una agencia creada por la vía ordinaria estaría operativa hacia 2030-2032. La amenaza no espera: el veto de IA ya ocurrió (junio 2026), las elecciones de 2029 ya estarán bajo IA generativa avanzada	

Los cuatro tipos de cuello de botella

- **Políticos:** unanimidad en el Consejo para lo sensible; intereses nacionales divergentes (Francia regulatoria, Alemania autorregulatorio, solapamientos de soberanía nacional). La cooperación reforzada (TFUE art. 326-334) existe precisamente para saltarse este bloqueo.
- **Legales:** el procedimiento legislativo ordinario tarda años; las competencias en educación y cultura son nacionales, lo que bloquea programas europeos de alfabetización mediática a gran escala.

- **Administrativos:** contratar talento de IA en un organigrama de la UE exige procedimientos que el sector privado resuelve en semanas; los mejores perfiles eligen otros destinos.
- **Técnicos:** escasez de expertos en detección de deepfakes y análisis de campañas; infraestructura propia insuficiente (Cap. 4) justo cuando la detección se vuelve carga de cómputo intensiva.

5.4 El European Democracy Shield (2025): el diagnóstico oficial y su límite

El 12 de noviembre de 2025 la Comisión Europea y el Alto Representante publicaron la comunicación conjunta **"The European Democracy Shield: Empowering Strong and Resilient Democracies"**. Es la respuesta institucional más ambiciosa hasta la fecha al diagnóstico de esta Parte I — y su lectura atenta confirma exactamente la tesis de este libro.



La crítica verificada: coordinar no es proteger

El análisis del **Jacques Delors Centre** (diciembre 2025) —"papering over the cracks", parchear las grietas— resume el límite estructural del Escudo:

- El nuevo **Centro Europeo de Resiliencia Democrática** es una **estructura de coordinación basada en la participación voluntaria de los Estados**: reúne experiencia existente, no construye capacidad nueva.
- Se parece sospechosamente al **Rapid Alert System** del EEAS (2019), montado para las elecciones europeas de aquel año — y que **"nunca despegó"**, según el balance retrospectivo de 2025.
- Riesgo verificado de **duplicar estructuras** sin claridad sobre qué añade el Centro a lo existente (EDMO, East StratCom, unidades nacionales).
- El Escudo se apoya en presupuestos propuestos del próximo marco financiero (CERV+ €3.600M, AgoraEU €8.600M) que aún requieren negociación y despliegan sobre todo **subvenciones a terceros**, no capacidad operativa propia.

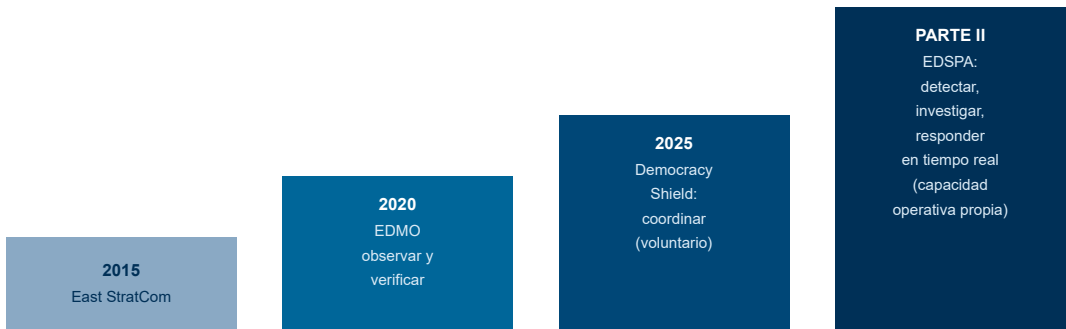
El límite que funda la Parte II

El European Democracy Shield es la prueba institucional de que la UE **ya acepta este diagnóstico**: hay una amenaza, es transnacional, y requiere respuesta europea. Lo que el Escudo no puede dar —por diseño— es lo que el Rapid Alert System tampoco pudo dar en 2019: **capacidad operativa permanente**. Detección temprana propia. Investigación propia. Respuesta en tiempo real propia. Un centro que coordina voluntariamente a los que ya existen no cierra el hueco identificado en 5.2: es su continuación burocrática. La EDSA de la Parte II es el siguiente peldaño lógico — y este capítulo lo argumenta con las fuentes oficiales de la propia UE.

5.5 El caso para una protección dedicada: la EDSPA

La escalera de la respuesta europea

De observar a proteger: los peldaños de la respuesta europea



Cada peldaño añadió alcance pero ninguno cerró el hueco: nadie "opera". La escalera tiene un peldaño más — y este libro lo diseña.

Figura 5.4 — La evolución de la respuesta europea: de monitorear a coordinar. Falta operar.

Por qué la protección cognitiva necesita una institución dedicada

Sector crítico	Amenaza	Institución especializada	Escala de recursos
Seguridad exterior	Guerra, terrorismo	OTAN, agencias nacionales	Trillones de euros acumulados
Fronteras físicas	Tráfico, migración irregular	Frontex (~€1.100M/año; propuesta €11.900M 2028-2034)	Centenas de millones anuales
Ciberseguridad	Ciberataques	ENISA (€26,9M/año) + CERTs nacionales	Decenas de millones
Protección cognitiva	Manipulación digital de masas	Ninguna con capacidad operativa (solo observación y coordinación)	Unidades de €2,5-11M

El presupuesto de referencia: una agencia operativa de protección cognitiva requeriría, en la estimación ilustrativa de este autor, **€500-1.000M anuales** — el orden de magnitud de Frontex para la frontera física (~€1.100M verificados en 2025). Es la escala a la que Europa ya protege una frontera bajo ataque; la frontera cognitiva merece al menos la misma lógica presupuestaria. (*Estimación ilustrativa del autor; los cálculos detallados de costes y retornos de la EDSPA se desarrollan en los capítulos 9 y 9B.*)

Cómo arrancarla: la cooperación reforzada

El análisis de cuellos de botella (5.3) desaconseja esperar el consenso de los 27. La **cooperación reforzada** (TFUE, art. 326-334) permite que un grupo de Estados Miembros —al menos nueve— cree la agencia sin esperar a todos, como ya hicieron el euro, la unión de patentes o el divorcio europeo. Es la vía que la Parte II propone para el arranque de la EDSPA, con la puerta abierta a que el resto se adhiera después.

Los cinco argumentos de la urgencia

- **La amenaza crece más rápido que la respuesta:** la IA generativa abarata cada año la manipulación; la ley necesita años (5.3).
- **El coste de la inacción es real:** economía de datos UE27 de €630.000M (4,7% del PIB, Cap. 4) construida sobre suelo que Europa no controla; erosión nacional de la confianza (Cap. 3); deslegitimación post-electoral verificada (EE.UU. 2020, Brasil 2022).
- **Las soluciones existentes se han probado y no bastan:** Rapid Alert System (2019, fallido), EDMO (€2,5M, observación), Escudo 2025 (coordinación voluntaria) — el propio Delors Centre lo certifica.

- **Europa tiene la capacidad:** supercomputación EuroHPC (JUPITER exaescala), Mistral AI, Cohere-Aleph Alpha, nube europea emergente (Cap. 4) — falta la institución que la orqueste.
- **El momento político es el mejor en años:** el veto de IA de junio de 2026 creó conciencia de dependencia; el Escudo 2025 puso el tema en el centro de la agenda; la propuesta de marco financiero 2028 incluye ya programas democráticos por decenas de miles de millones. La ventana está abierta — y las ventanas se cierran.

Datos y estadísticas del capítulo

Dato	Valor	Fuente
EDMO (unidad central)	€2,5M de financiación	Comisión Europea (Digital Europe)
East StratCom Task Force	~€11M y ~40 expertos (2022)	EEAS / documentación parlamentaria
ENISA (ciberseguridad)	€26,9M anuales (2025) + €36M Reserva Ciber	ENISA (2025)
Frontex (frontera física)	~€1.100M (2025); propuesta €11.900M 2028-2034	Frontex / Comisión Europea (2025)
European Democracy Shield	Comunicación conjunta 12-nov-2025; Centro Europeo de Resiliencia Democrática (coordinación voluntaria)	Comisión Europea / SEAE (2025)
Rapid Alert System	2019; "nunca despegó" según el balance retrospectivo	RFE/RL, Delors Centre (2025)
Presupuesto propuesto para la EDSPA	€500-1.000M/año (estimación ilustrativa del autor, ancla: Frontex)	Este libro (detallado en caps. 9 y 9B)
Duración verificada de la vía legislativa ordinaria	DSA ~4 años; AI Act ~6 años hasta aplicación plena	Proceso legislativo UE

Fuentes

- Comisión Europea / Alto Representante (12 de noviembre de 2025). *The European Democracy Shield: Empowering Strong and Resilient Democracies* — Comunicación conjunta.
- EPRS — European Parliamentary Research Service (2026). *The European Democracy Shield: An Overview*.
- Jacques Delors Centre (diciembre 2025). *The European Democracy Shield — Papering over the Cracks*.
- Comisión Europea. Financiación de EDMO y su red de 15 hubs (CEF / Digital Europe).
- EEAS / documentación parlamentaria alemana (2022). Datos de East StratCom Task Force y EUvsDisinfo.
- ENISA (2025). Presupuesto anual y EU Cybersecurity Reserve (€36M).
- Frontex (2024-2025). Presupuesto votado 2025; Comisión Europea, DG HOME (jul. 2025): propuesta de €11.900M para 2028-2034 (Statewatch cita €11.200M).
- Gobierno de Francia. Décret n° 2021-922 du 13 juillet 2021 (creación de Viginum).
- RFE/RL / Globalsecurity (noviembre 2025). Balance del Rapid Alert System y cobertura del Escudo.
- Vosoughi, S., Roy, D. y Aral, S. (2018). *Science* — base de la síntesis de amenazas (caps. 2 y 1-4).

Conexión con el resto del libro

La Parte I queda cerrada: la amenaza (caps. 1-3), la imposibilidad de defenderse con herramientas prestadas (cap. 4) y la insuficiencia demostrada de los mecanismos actuales —incluido el Democracy Shield de 2025— (cap. 5). La **Parte II** (capítulos 6-10 y 9B) construye la solución: la teoría del Poder Protector (cap. 6), la protección cognitiva como derecho (cap. 7), el mandato del Protector (cap. 8) y la EDSPA con su ROI y su impacto económico y social (caps. 9, 9B, 10). La **Parte III** (capítulos 11-20) la eleva a cuarto poder constitucional de Europa: el Poder Protector.

Capítulo 6: EDSPA — Fundamentos de la Agencia Europea de Protección de la Esfera Digital

Resumen del capítulo

Este capítulo abre la Parte II y establece los **fundamentos de la EDSPA** (European Digital Sphere Protection Agency), la agencia que operacionalizará el Poder Protector. Presenta su misión y valores, la **base legal** que permite crearla sin reforma del Tratado (mercado interior, protección de datos y, sobre todo, cooperación reforzada entre un mínimo de **nueve Estados**), un **núcleo fundador de nueve Estados Miembros** seleccionados con datos verificados de 2025, la propuesta de **sede en Bruselas** siguiendo el precedente de las relocalizaciones de la EMA y la EBA, una **financiación en tres escenarios** (€500M, €1.000M y un escenario acelerado de €2.500M coherente con el Capítulo 9) y los **principios fundamentales** que la gobernarán. La comparación es elocuente: la EDSPA propuesta operaría con el mismo orden de magnitud que Frontex (~€1.100M en 2025) para la frontera cognitiva.

6.1 ¿Qué es la EDSPA?

Definición y misión

EDSPA — *European Digital Sphere Protection Agency*; en español, Agencia Europea de Protección de la Esfera Digital; en francés, *Agence Européenne de Protection de la Sphère Numérique*; en alemán, *Europäische Agentur für den Schutz der digitalen Sphäre*.

«Proteger la esfera cognitiva digital de los ciudadanos, instituciones y sociedades europeas contra la manipulación, la desinformación y las amenazas algorítmicas, garantizando la soberanía digital, la autonomía cognitiva y la resiliencia democrática de la Unión Europea.»

Misión propuesta de la EDSPA

Su visión: ser el **referente global en protección cognitiva**, con un modelo replicable por otras democracias, basado en la transparencia, la ética y el respeto a los derechos fundamentales.

Objetivos estratégicos

Objetivo	Contenido
1. Protección cognitiva	Detectar y neutralizar campañas de desinformación y manipulación; proteger frente a la influencia algorítmica no ética; garantizar la integridad de los procesos democráticos
2. Soberanía digital	Reducir la dependencia tecnológica; promover la tecnología europea en IA y protección digital (Mistral AI, valoración ~€11.700M en 2026, como activo de referencia); asegurar control europeo sobre datos e infraestructura crítica
3. Resiliencia democrática	Fortalecer la capacidad de la UE frente a interferencias externas; proteger la libertad de expresión y el pluralismo informativo; garantizar transparencia y responsabilidad de las plataformas
4. Cooperación internacional	Establecer estándares globales de protección cognitiva; colaborar con otras democracias; exportar el modelo a países aliados

Valores fundamentales

Valor	Aplicación en la EDSPA
Transparencia	Informes públicos, auditorías externas, datos abiertos (cuando sea seguro)
Independencia	Contratación por mérito, mandatos limitados, financiación diversa
Excelencia	Los mejores expertos, formación continua, evaluación rigurosa
Ética	Cumplimiento estricto del RGPD, la Carta de Derechos Fundamentales y los principios de IA ética
Colaboración	Coordinación con Estados Miembros, plataformas, sociedad civil y academia
Innovación	Inversión en I+D, adopción de IA ética, herramientas propias
Rendición de cuentas	Mecanismos de supervisión, evaluaciones independientes, transparencia en decisiones

6.2 Base legal: crear la EDSPA sin reforma del Tratado

La EDSPA puede crearse **sin necesidad de reforma del Tratado de la UE**, combinando cuatro bases legales existentes:

1. Mercado interior (artículo 114 TFUE)

La fragmentación de la protección cognitiva entre Estados Miembros **distorsiona el mercado interior digital**: la desinformación erosiona la confianza en el mercado digital común y la ausencia de estándares comunes crea barreras al comercio y la innovación. El artículo 114 permite adoptar **reglamentos vinculantes** para toda la UE — la misma vía por la que se aprobaron el RGPD, el DSA y el AI Act.

2. Protección de datos personales (artículo 16 TFUE)

La protección cognitiva está íntimamente ligada a la protección de datos: la manipulación algorítmica se apoya en el uso no ético de datos personales. Es una base legal **ya establecida y probada**, articulada con el RGPD y la futura aplicación plena del AI Act (obligaciones de transparencia sintética aplicables desde agosto de 2026).

3. Cooperación reforzada (artículos 20 TUE y 326-334 TFUE)

La vía de arranque. El artículo 20 TUE permite a un grupo de Estados Miembros **avanzar sin necesidad de consenso de los 27**, utilizando las instituciones de la Unión. El requisito mínimo verificado: la cooperación reforzada debe agrupar al menos **nueve Estados Miembros**. Es ideal para la fase inicial con un núcleo fundador y puede expandirse gradualmente. El precedente existe: la cooperación reforzada ya se ha usado en materia de divorcio, propiedad intelectual unitaria o el MEPC (protección penal del euro). Evita el bloqueo por parte de Estados reticentes.

4. Competencias de apoyo (artículo 6 TFUE)

La UE puede realizar acciones de apoyo, coordinación o complemento en áreas como la educación, la cultura y la protección de los consumidores. La alfabetización mediática y la protección del «consumidor cognitivo» encajan en este marco sin invadir competencias nacionales.

De la propuesta a la operación

Creación de la EDSPA: 18-30 meses, sin reforma del Tratado



Estructura legal: agencia descentralizada de la UE (similar a ENISA, EMA o Frontex), con personalidad jurídica propia y autonomía administrativa y financiera, creada por reglamento del Parlamento Europeo y del Consejo, con reglamento interno, decisiones del consejo directivo y acuerdos con Estados Miembros para la implementación nacional.

Por qué la base legal es creíble

El AI Action Summit de febrero de 2025 y el programa **InvestAI** (movilización de €200.000M para IA en Europa, incluidos €20.000M para gigafábricas de IA) demostraron que la UE sabe activar instrumentos financieros de gran escala en meses. La creación de una agencia por reglamento es una técnica institucional madura: la UE cuenta hoy con más de 30 agencias descentralizadas. La EDSPA no inventaría nada en derecho institucional; aplicaría lo existente a un dominio nuevo.

La demanda institucional ya existe

Antes de cualquier propuesta de este libro, la propia Comisión ha ido construyendo — con instrumentos frágiles — la función que la EDSPA consolidaría: cuatro rondas consecutivas de la línea «European Narratives Observatory» de DG CNECT (NODES 2022; 2ª call 2023 sobre Ucrania, desinformación de género y elecciones; 3ª call 2025 «Detecting influence campaigns and boosting societal resilience», dos proyectos de €1,5M y €1,65M; piloto PPPA-2026 de cohesión social, €785.000), el consorcio SHIFT (arranque abril-2026, 18 meses, 13 países) y el European Centre for Democratic Resilience del Democracy Shield (intergubernamental, sin autoridad, en marcha desde el 24-feb-2026). La Comisión admite que necesita anticipar, detectar y responder a escala — pero lo construye sin poder, con proyectos que expiran. La EDSPA es el siguiente paso lógico: mismo mandato, con independencia, permanencia y competencias.

6.3 El núcleo fundador: nueve Estados Miembros

La cooperación reforzada exige un mínimo de **nueve Estados Miembros**. Proponemos exactamente ese núcleo inicial: un grupo con masa crítica económica, tecnológica y política, seleccionado con criterios verificables.

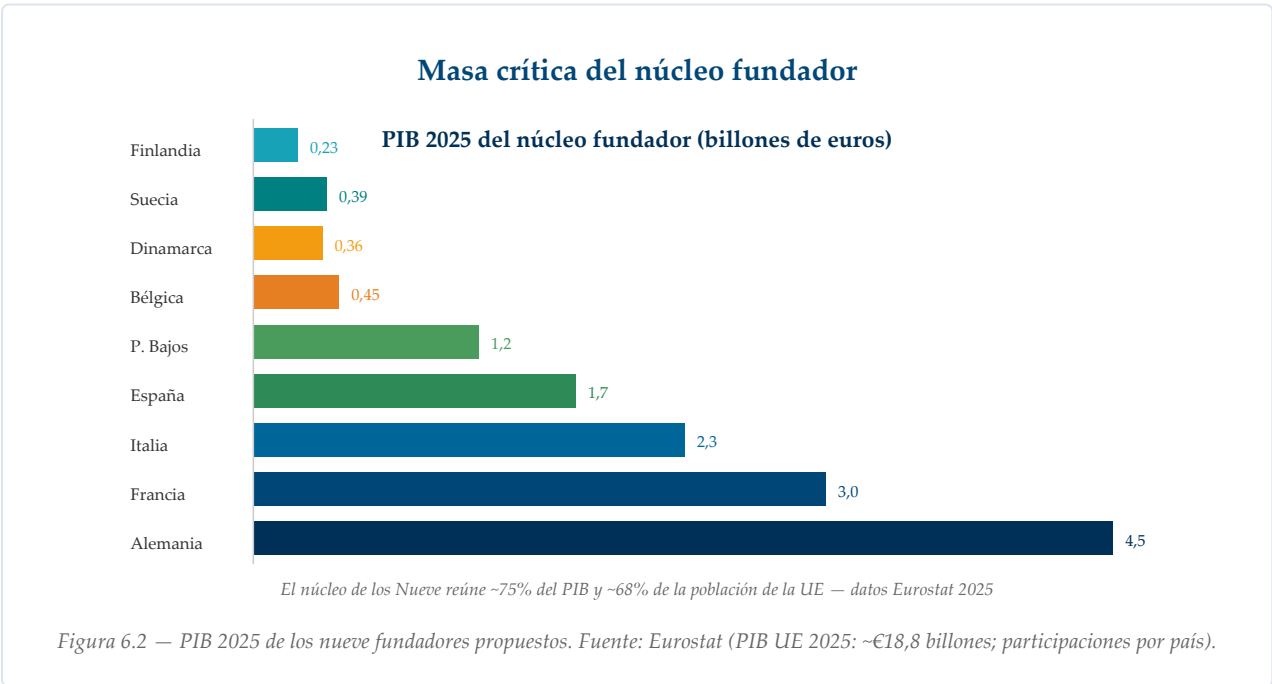
Criterios de selección

- **Compromiso político:** voluntad gubernamental clara y apoyo a los valores de la EDSPA

- **Capacidad técnica:** infraestructura digital, supercomputación (EuroHPC), expertos en IA y ciberseguridad
- **Capacidad financiera:** contribución al presupuesto proporcional al PIB y financiación de nodos nacionales
- **Marco legal compatible:** legislación nacional aplicable y protección de derechos fundamentales garantizada

El núcleo de los Nueve (datos 2025 verificados)

País	PIB 2025	Población	Activos clave	Justificación
Alemania	~€4,5 billones (~24% del PIB UE)	84M	JUPITER (supercomputación exaescala, Jülich); GAIA-X	Primera economía de la UE; masa crítica industrial y de investigación
Francia	~€3,0 billones (~16%)	68M	Mistral AI (~€11.700M de valoración); €109.000M comprometidos en IA (AI Action Summit 2025)	Líder europeo en IA frontera y en computación soberana
Italia	~€2,3 billones (~12%)	59M	Leonardo; hub de HPC (Bologna)	Tercera economía de la UE; compromiso político
España	~€1,7 billones (~9%)	47M	BSC / MareNostrum 5 (Barcelona)	Líder en supercomputación; compromiso con la protección cognitiva
Países Bajos	~€1,2 billones (~6,3%)	17M	AMS-IX, ecosistema de HPC; sede de Europol y EMA	Hub digital de Europa; sede de la EMA desde 2019
Bélgica	~€0,45 billones	11M	Sede de las instituciones de la UE; dark fiber y datacenters	Candidata natural a sede central
Suecia	~€0,39 billones	10M	Ecosistema tecnológico nórdico; nodos de datos sostenibles	Líder en innovación digital y valores democráticos
Finlandia	~€0,23 billones	5,5M	LUMI (uno de los superordenadores más potentes de Europa, Kajaani)	Referente en ética digital; experiencia en protección de infraestructura electoral
Dinamarca	~€0,36 billones	5,8M	Digitalización avanzada del sector público; centros de datos verdes	Líder en digitalización y protección de datos
Total núcleo de los 9	~€14,1 billones (~75% del PIB UE de ~€18,8 billones)	~307M (~68% de la población UE)	3 de los grandes superordenadores EuroHPC	Masa crítica suficiente para lanzar la cooperación reforzada



Proceso de adhesión de nuevos Estados

1. **Expresión de interés** (3 meses): carta formal del gobierno al consejo directivo y evaluación inicial de elegibilidad
2. **Evaluación técnica** (6 meses): auditoría de capacidad, compatibilidad legal, análisis financiero
3. **Negociación** (3-6 meses): acuerdo de adhesión, plan de implementación, compromisos financieros
4. **Aprobación** (2 meses): recomendación del consejo directivo y aprobación por mayoría cualificada
5. **Implementación** (6-12 meses): nodo nacional, contratación, integración en sistemas, formación

Tiempo total estimado: 12-24 meses desde la expresión de interés hasta la plena operación. Objetivos de expansión: 20 Estados Miembros en 2028, los 27 en 2030.

6.4 Sede central e infraestructura

El precedente institucional

La UE tiene un procedimiento probado para decidir sedes: tras el Brexit, los Veintisiete votaron en 2017 la relocalización de la **EMA a Ámsterdam** y la **EBA a París**, y los reglamentos fundacionales se enmendaron en consecuencia. La sede de una agencia nueva se decide por los Estados Miembros, no por la Comisión — y las candidaturas se negocian con ofertas de incentivos del país anfitrión.

Criterios y evaluación comparativa

Criterio	Alemania	Francia	España	Bélgica	P. Bajos	Suecia	Finlandia
Centralidad geográfica	9	8	7	10	9	6	5
Infraestructura digital	10	9	8	9	10	9	8
Capacidad técnica	10	9	8	8	9	8	7
Estabilidad política	9	8	8	9	9	10	10
Costes e incentivos	7	6	9	8	7	6	7
Total (máx. 50)	45	40	40	44	44	39	37

Recomendación: Bruselas (Bélgica), con Ámsterdam como alternativa fuerte. Bruselas ofrece proximidad a la Comisión, el Consejo y el Parlamento Europeo (además de OTAN y OCDE), conectividad de primer nivel y un entorno naturalmente multilingüe. La decisión final corresponde, como en el precedente EMA/EBA, a los Estados Miembros.

Infraestructura de la sede

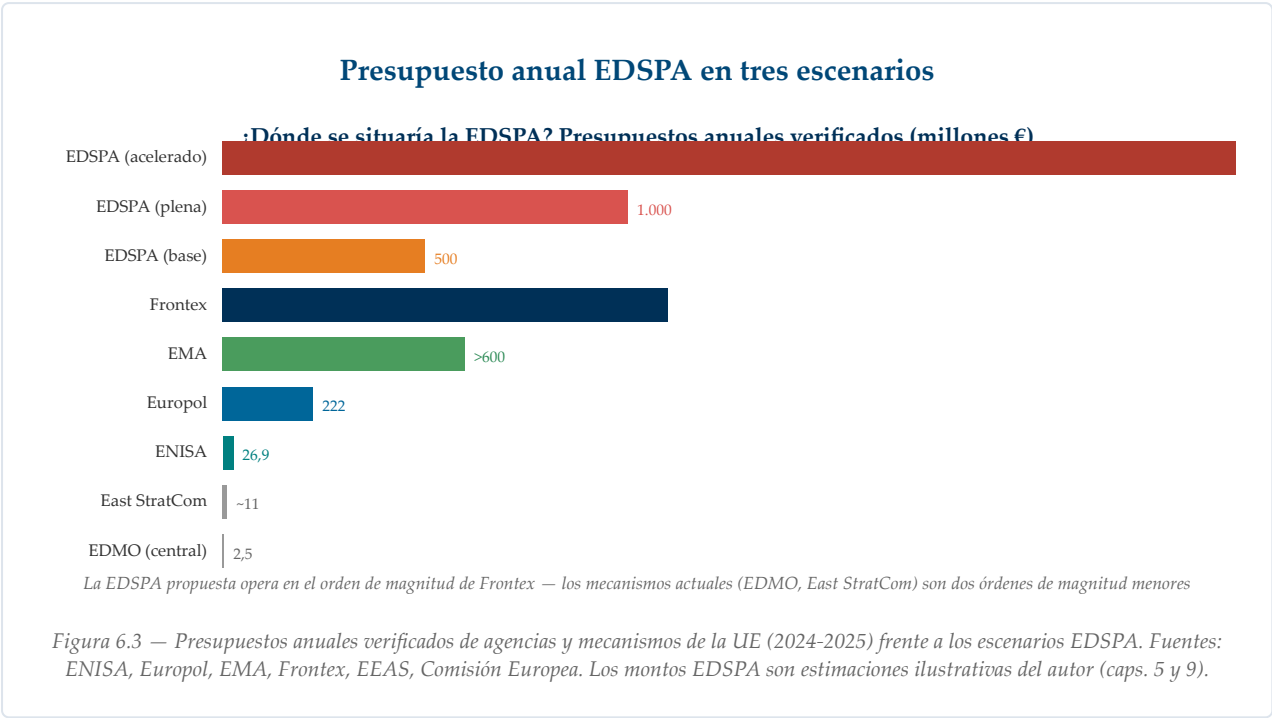
- **Edificio principal:** ~50.000 m² — oficinas para 1.000-1.500 empleados, datacenter en sede (10.000 m²), laboratorios de IA y análisis (5.000 m²), sala de crisis 24/7 (1.000 m²), auditorio y zonas comunes
- **Computación:** la EDSPA no necesita construir supercomputación desde cero: puede apoyarse en **EuroHPC** (JUPITER, LUMI, MareNostrum 5) con capacidad dedicada, más un clúster propio de GPU para análisis en tiempo real
- **Datacenter principal** (~€500M): co-ubicación en Bélgica o Países Bajos, energía 100% renovable, redundancia N+2, certificación ISO 27001 y estándares de la ENISA
- **Datacenter de respaldo** (~€450M) en Ámsterdam/Fráncfort + red propia (~€100M) con conexión a GÉANT

Nota de rigor: las cifras de datacenter y red (~€850M en total) son **estimaciones ilustrativas del autor** para una infraestructura de misión crítica con redundancia geográfica; no proceden de ningún presupuesto oficial. El anclaje realista disponible: JUPITER, el primer superordenador exaescala europeo, ha supuesto ~€500M, lo que confirma el orden de magnitud. La opción EuroHPC (capacidad dedicada en lugar de infraestructura propia) podría reducir la inversión inicial de forma sustancial.

6.5 Financiación: tres escenarios coherentes

El Capítulo 5 fijó el rango de referencia para la EDSPA — **€500-1.000M al año**, estimación ilustrativa anclada en Frontex (~€1.100M en 2025 para la frontera física) — y el Capítulo 9 añade un **escenario acelerado de €2.500M**

con 2.000 empleados. Este capítulo estructura ese rango en escenarios con fuentes verificables:



Escenario	Presupuesto anual	Personal	Vía de financiación dominante	Referencia
Base	€500M	~1.000-1.500	Cooperación reforzada de los Nueve + programas UE (Horizon Europe €93.500M / Digital Europe €8.100M 2021-2027)	Ancla: media de ENISA-Europol-EMA-Frontex
Plena	€1.000M	~3.000-5.000	Aportaciones de los 27 (referencia Frontex ~€1.100M para misión crítica)	Ancla: Frontex 2025
Acelerado	€2.500M	~2.000 empleados (sede) + nodos nacionales	Puesta en marcha 2026-2027 con instrumentos tipo InvestAI (€200.000M movilizables para IA)	Coherente con Cap. 9

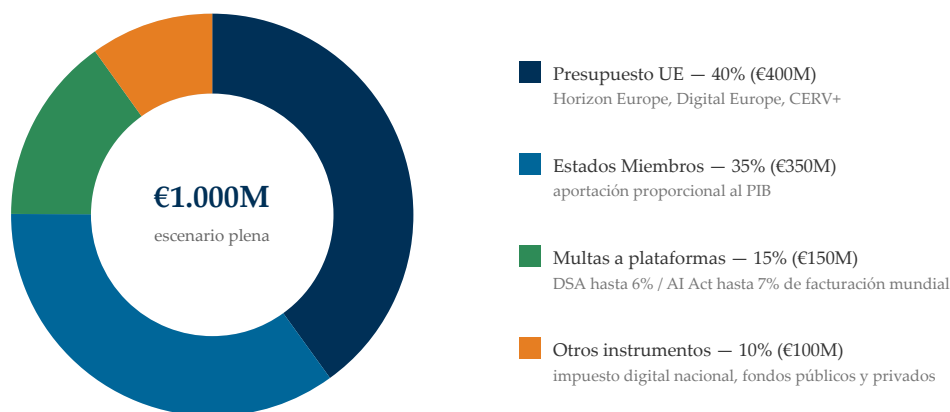
Los tres escenarios son estimaciones ilustrativas del autor, ancladas en presupuestos reales verificados de agencias de la UE

Estructura de fuentes (escenario plena, €1.000M)

Fuente	Mecanismo	Aportación anual	%
Presupuesto de la UE	Horizon Europe, Digital Europe, CERV+ (€3.600M, Democracy Shield)	€400M	40%
Estados Miembros	Aportación proporcional al PIB (~0,003-0,005% del PIB de los 27)	€350M	35%
Multas a plataformas	Destino específico de sanciones DSA (hasta 6% de facturación mundial) y AI Act (hasta 7% / €35M)	€150M	15%
Otros instrumentos	Impuesto digital nacional complementario, fondos públicos y privados	€100M	10%
Total		€1.000M	100%

Estructura de financiación (escenario plena, €1.000M)

¿De dónde vendría el presupuesto anual de €1.000M?



Financiación diversa = garantía de independencia (sección 6.6); ninguna fuente supera el 40%

Figura 6.4 — Estructura de fuentes del escenario plena. Elaboración del autor; estimación ilustrativa anclada en programas UE verificados.

Inversión inicial (2027-2028)

Concepto	Coste estimado	Financiación
Sede central (Bruselas) y equipamiento	€200M	UE (50%) / fundadores (50%)
Capacidad dedicada EuroHPC + nube europea soberana (contratos plurianuales)	€250M	UE (50%) / fundadores (50%)
Red propia + GÉANT y despliegue de nodos nacionales	€100M	UE (100%)
Personal (despliegue inicial, 1.500 empleados, Cap. 7)	€150M	UE (40%) / fundadores (60%)
Herramientas propias de detección y auditoría (Cap. 8)	€200M	Fondos UE y de inversión
Formación y capacidades nacionales	€50M	UE (100%)
Arranque de alfabetización mediática y comunicación	€70M	UE (100%)
Reserva de contingencia	€80M	Todas las fuentes
Total inversión inicial	€1.100M	

Coherencia con los Capítulos 9 y 9B: este desglose es el escenario base (€1.100M, 2027-2028), sin datacenters propios — capacidad dedicada en EuroHPC + nube europea, según el consenso de costes de la Parte II. El escenario acelerado (€2.500M, 2026-2027) adelanta el mismo modelo (Cap. 9). La infraestructura propia de datacenters se retoma como evolución futura del Poder Protector (Cap. 17).

6.6 Principios fundamentales de la EDSPA

1. Independencia absoluta

Contratación por mérito con procesos transparentes; mandatos directivos de 4-8 años no renovables automáticamente; financiación diversa (sección 6.5) para evitar dependencias; veto de conflictos de interés con plataformas, gobiernos extranjeros o intereses corporativos, con declaración pública de intereses.

2. Excelencia técnica

Área	Perfil	Rango salarial anual (€)
IA y aprendizaje automático	Deep learning, PLN, visión por computadora	120.000-180.000
Ciberseguridad	Detección de intrusiones, análisis forense	110.000-160.000
Análisis de datos	Big data, estadística, visualización	100.000-150.000
Derecho digital	RGPD, DSA, AI Act, propiedad intelectual	100.000-140.000
Desinformación	Análisis de narrativas, verificación	90.000-130.000
Ética de la IA	Impacto social, sesgos, transparencia	90.000-120.000

Rangos de referencia del mercado tecnológico europeo para perfiles senior; la EDSPA los complementaría con estabilidad, misión de interés público y formación continua — el mismo equilibrio que permite a Europol (~1.400 empleados) o la EMA atraer talento.

3. Transparencia radical

Informes públicos periódicos; auditorías externas (Tribunal de Cuentas); datos abiertos agregados y anonimizados; consultas públicas. Límites: operaciones en curso, privacidad (RGPD) y secretos comerciales.

4. Cooperación internacional

Acuerdos bilaterales con democracias (Reino Unido, Canadá, Australia, Japón, Corea del Sur); participación en ONU, OCDE y OTAN; exportación del modelo con estándares globales. Límite innegociable: **prohibición absoluta de compartir información o tecnología con regímenes no democráticos**, y control europeo sobre las decisiones críticas.

5. Rendición de cuentas

KPI	Objetivo 2027	Objetivo 2030
Tiempo de detección de desinformación	< 6 horas	< 2 horas
Tasa de acierto en verificación	> 90%	> 95%
Campañas neutralizadas (por año)	500	2.000
Satisfacción de Estados Miembros	> 80%	> 90%
Satisfacción ciudadana	> 70%	> 80%
Presupuesto ejecutado	> 90%	> 95%

6.7 Conclusión: la EDSPA como paso estratégico

La Parte I demostró que la amenaza cognitiva es real, creciente y transversal, y que los mecanismos actuales — EDMO con €2,5M, East StratCom con ~€11M y 40 expertos, el Democracy Shield sin capacidad operativa propia — son dos órdenes de magnitud menores que lo que requiere el problema. Este capítulo ha demostrado que la respuesta institucional es **viable sin reforma del Tratado** (cooperación reforzada de nueve Estados), **financiable** (el rango €500-1.000M es el orden de magnitud de lo que la UE ya gasta en Frontex), y **gobernable** con principios de independencia, excelencia, transparencia y rendición de cuentas.

El veto de IA estadounidense de junio de 2026 (Cap. 4) demostró que la dependencia es una vulnerabilidad; la capacidad nacional de Francia (Mistral AI, €109.000M comprometidos) y la infraestructura EuroHPC del núcleo fundador demuestran que Europa tiene los activos. Lo que falta no es tecnología ni dinero: es la **institución** que los orqueste. La EDSPA es esa institución.

Próximos pasos: el Capítulo 7 desarrollará la estructura organizacional completa (consejo directivo, organigrama, departamentos técnicos y administrativos, procesos de contratación) y el Capítulo 8 las operaciones y procesos (detección, análisis, respuesta, doble verificación humana e IA, nodos nacionales, evaluación).

Fuentes verificadas de este capítulo

- Eurostat (2025): PIB de la UE ~€18,8 billones; Alemania ~24%, Francia ~16%, Italia ~12%, España ~9%, Países Bajos ~6,3%, Polonia ~5%
- ENISA: presupuesto 2025 de €26,9M; €36M adicionales para la Reserva de Ciberseguridad de la UE (2025)
- Europol: presupuesto 2024 de €222,4M; ~1.400 empleados (La Haya)
- EMA: presupuesto 2025 superior a €600M (nueva normativa de tasas); sede en Ámsterdam desde 2019
- Frontex: ~€1.100M en 2025 (Cap. 5); cuerpo permanente previsto de 10.000 efectivos para 2027
- Artículo 20 TUE: cooperación reforzada con un mínimo de nueve Estados Miembros
- Comisión Europea: relocalización de la EMA (Ámsterdam) y la EBA (París), procedimiento de los Veintisiete, 2017-2018
- DSA: sanciones de hasta el 6% de la facturación mundial anual; AI Act: hasta el 7% o €35M para prácticas prohibidas
- Horizon Europe: €93.500M (2021-2027); Digital Europe Programme: €8.100M (2021-2027)
- InvestAI (Comisión Europea, feb. 2025): €200.000M movilizados para IA, incluidos €20.000M para gigafábricas; Francia: €109.000M comprometidos (AI Action Summit, feb. 2025)
- JUPITER (supercomputador exaescala EuroHPC, Jülich, ~€500M), LUMI (Kajaani), MareNostrum 5 (BSC, Barcelona)

Capítulo 7: Estructura Organizacional de la EDSPA

Resumen del capítulo

La EDSPA no puede ser una agencia más de la UE. Este capítulo diseña su estructura organizacional sobre el principio de **mínima injerencia estatal en la sede central**: un **Consejo de Protectores** de 17 expertos independientes elegidos por mérito — sin un solo representante de los Estados — siguiendo el modelo que el **Consejo Científico del ERC** ha demostrado durante casi dos décadas, con la independencia funcional y financiera que el **BCE** aporta al derecho institucional europeo. Los Estados Miembros no desaparecen del mapa: se integran en un **Consejo Asesor sin voto** en la sede y en una **Cámara Nacional** de coordinación en los nodos territoriales, bajo un modelo dual (eu-LISA + EDPB) que reserva toda la dirección operativa a la central. El capítulo detalla la dirección ejecutiva, los seis departamentos, la distribución de personal y presupuesto del escenario base (€500M, 1.500 empleados) y un sistema de **garantías sin fricción**: contrapesos de rendición de cuentas diseñados para que ni los Estados ni los litigantes corporativos puedan frenar la operación.

7.1 La tesis: protección cognitiva = política monetaria, no política de foso

¿Por qué una agencia de protección cognitiva no puede gobernarse como Frontex o Europol? Porque su objeto de trabajo es **la mente de los ciudadanos**, el terreno donde precisamente se libran las batallas de interferencia que la Parte I documentó. Una agencia cuyo consejo directivo esté formado por un representante por Estado es una agencia donde cada gobierno de turno — incluidos los que hoy patrocinan medias verdades en su propio beneficio electoral — tiene asiento, voz y voto sobre quién protege a los ciudadanos y contra quién.

«Nadie propone que los gobiernos nacionales nombren a los miembros del consejo del BCE. La independencia del banco central se considera condición de su eficacia. La protección cognitiva merece exactamente la misma arquitectura: quien vigila la esfera pública de ideas no puede depender del poder político que opera dentro de ella.»

Tesis central del capítulo

El riesgo verificado: la UE ya ha vivido lo que ocurre cuando el poder político se inmiscuye en un organismo con mandato técnico. En 2022, el Consejo y el Parlamento enmendaron el reglamento de Europol para **legalizar retroactivamente** prácticas de retención masiva de datos que el EDPS había ordenado cesar — y el intento del supervisor europeo de anular esas disposiciones fue declarado inadmisibile (caso T-578/22). La lección para la EDSPA: la independencia que no está **blindada en el reglamento fundacional** puede ser desmontada en una sola ronda de negociación presupuestaria.

El gradiente de independencia de los organismos de la UE

Los organismos europeos forman un gradiente medible de injerencia estatal. Las agencias estándar (ENISA, Europol, EUIPO, eu-LISA) tienen consejos con un representante por Estado Miembro más la Comisión. El EDPB está compuesto por autoridades nacionales *independientes* — reguladores, no gobiernos. Y en el extremo de máxima independencia están el **ERC** (Consejo Científico de ~22 expertos por mérito, cero representación estatal, la mejor reputación de excelencia de la UE), el **BCE** (cinco pilares de independencia institucional) y el **EDPS** (supervisor único, sin junta estatal). La EDSPA propuesta se sitúa deliberadamente en ese extremo.

¿Dónde se sitúa cada organismo?

El gradiente de injerencia estatal en los órganos de gobierno



¿Por qué el extremo independiente?

- El ERC: ~22 expertos por mérito, cero representantes estatales — la institución europea con mejor reputación de excelencia y quince Premios Nobel entre sus financiados
- El BCE: prohibición de instrucciones a los órganos, mandatos largos, financiación propia
- El precedente Europol 2022: sin blindaje, el legislador desmonta garantías en una ronda
- La EDSPA vela por la esfera donde la interferencia política es la amenaza, no la solución

Figura 7.1 — El gradiente de injerencia estatal en los organismos de la UE. Elaboración propia sobre la composición verificada de cada consejo rector (ENISA, Europol, EUIPO, eu-LISA, Frontex, EDPB, BCE, EDPS, ERC).

7.2 El órgano de gobierno: Consejo de Protectores

Composición (modelo ERC)

El **Consejo de Protectores** es el órgano rector de la EDSPA: **17 expertos independientes**, elegidos exclusivamente por mérito, **sin representación estatal alguna**. Ningún gobierno designa, vet ni remueve a sus miembros.

Puesto	Número	Selección	Mandato
Miembros por mérito	17	Convocatoria abierta en toda la UE + comité de selección independiente (procedimiento verificado del tipo Europol 2026: evaluación, entrevistas, lista corta de al menos 3 candidatos) + confirmación por el propio Consejo	6 años, no renovable, renovación escalonada por tercios cada 2 años
— de los cuales, presidente/a	1	Elegido por y entre los 17 miembros	2 años renovable 1 vez dentro de su mandato
Comisión Europea	1 observador	Sin voto: coordinación institucional y presupuestaria	—
Parlamento Europeo	1 observador	Sin voto: voz del interés ciudadano	—
Estados Miembros	Consejo Asesor (sin voto)	Un representante por Estado, con voz en materia de nodos nacionales y prioridades territoriales	—
Miembros con derecho a voto	17 — 0 Estados	Todas las decisiones estratégicas, presupuestarias y de dirección	

Perfiles requeridos y prohibiciones

- **Composición multidisciplinar garantizada en el reglamento:** al menos 3 expertos en IA/algoritmos, 2 en ciberseguridad, 3 en derecho fundamental y digital, 2 en ciencias sociales/comportamiento, 2 en periodismo/medios, 2 en seguridad electoral, 1 en ética, 2 libres por evolución de la amenaza
- **Barreras de conflicto de interés** (más estrictas que cualquier agencia actual): veto total a vínculos con plataformas, gobiernos extranjeros o intereses corporativos; declaración pública de intereses; **cuarentena de 2 años** para ex-empleados de plataformas o ex cargos políticos nacionales con cartera digital
- **Diversidad obligatoria:** equilibrio de género (máximo 10/17 de un mismo género) y geográfico (máximo 2 miembros por Estado, sin cuotas nacionales: la nacionalidad es un dato, no un criterio)

Funciones del Consejo de Protectores

Ámbito	Funciones
Estratégicas	Aprobar el plan estratégico plurianual y las prioridades anuales; adoptar el presupuesto (dentro del marco plurianual blindado, sección 7.6); aprobar el programa de auditorías algorítmicas
De dirección	Nombrar y, en su caso, remover al Director Ejecutivo (con causa y procedimiento reglado); nombrar al Oficial de Derechos Fundamentales; aprobar los informes públicos anuales
De garante	Verificar el cumplimiento de los valores fundacionales; aprobar la revisión anual de código ético; responder ante el Parlamento Europeo y la opinión pública — nunca ante gobiernos individuales

Por qué 17 y no 27: un órgano de 27 miembros con representación estatal es un órgano donde el cálculo diplomático sustituye al mérito. El ERC funciona con ~22 expertos. Diecisiete es el tamaño mínimo que permite cubrir todos los perfiles técnicos con renovación escalonada por tercios (cada 2 años se renuevan 5-6 sillas sin descapitalizar el conocimiento acumulado) y el máximo que permite una deliberación real en sesión plenaria. Ningún asiento es «de» ningún país.

7.3 Dirección Ejecutiva

El **Director Ejecutivo** dirige la agencia en el día a día: implementación del plan estratégico, gestión de crisis, portavocía y asignación interna del presupuesto. Es nombrado por el Consejo de Protectores entre la lista corta de un comité de selección independiente — el mismo procedimiento abierto que la UE ya aplica para directores ejecutivos de agencias, verificado en el proceso Europol 2026: convocatoria pública, comité de selección del consejo, entrevistas y assessment center, lista corta de al menos 3 candidatos.

Puesto	Mandato	Reporta a
Director/a Ejecutivo/a	5 años, renovable 1 vez	Consejo de Protectores
Director/a de Operaciones (detección, auditoría, protección electoral)	4 años	Dirección Ejecutiva
Director/a de Tecnología (IA, infraestructura, soberanía)	4 años	Dirección Ejecutiva
Director/a de Asuntos Legales y Garantías	4 años	Dirección Ejecutiva
Director/a de Educación y Resiliencia	4 años	Dirección Ejecutiva
Oficial de Derechos Fundamentales (independiente)	5 años no renovable	Consejo de Protectores directamente (precedente Frontex)

Organigrama de la EDSPA

Estructura en 4 niveles: deliberación por mérito, ejecución profesional



Escenario base: 1.500 empleados en la sede y nodos; el detalle de equipos por departamento se conserva del diseño operativo original

Figura 7.2 — Organigrama de la EDSPA. La Oficina de Derechos Fundamentales reporta directamente al Consejo de Protectores, no a la cadena de mando operativa (precedente Frontex, reglamento 2019/1896).

7.4 Departamentos técnicos y administrativos

1. Detección y Análisis (330 empleados)

Los ojos de la EDSPA. Tres equipos: **IA** (150: modelos propios de detección de desinformación, deepfakes y contenido sintético), **Análisis de Datos** (100: procesamiento a gran escala, telemetría de plataformas) e **Inteligencia** (80: análisis de actores y campañas coordinadas, OSINT). Detección en tiempo real, identificación de patrones de manipulación, alertas tempranas. Personal máximo de todo el organigrama: la agencia es, ante todo, una máquina de percibir.

2. Auditoría Algorítmica (200 empleados)

La voz de la transparencia. Tres equipos: **Auditoría Técnica** (120: inspección de sistemas de recomendación y modulación de alcance, análisis estático y dinámico de algoritmos), **Legal** (50: DSA, AI Act, RGPD) y **Cumplimiento** (30: seguimiento de recomendaciones). Realiza auditorías independientes a las plataformas, evalúa el cumplimiento normativo, emite recomendaciones y publica informes públicos. Es el brazo que convierte la evidencia del Cap. 4 (recomendaciones algorítmicas que amplifican la falsedad) en obligación de corrección.

3. Protección Electoral (200 empleados)

El escudo de la democracia. Tres equipos: **Monitoreo** (100: vigilancia 24/7 en periodos electorales), **Respuesta Rápida** (60: neutralización en tiempo real de interferencias, bots, deepfakes) y **Coordinación** (40: enlace con autoridades electorales nacionales). Detección de interferencia extranjera, informes post-electorales públicos.

4. Educación Cognitiva (190 empleados)

El constructor de resiliencia. Tres equipos: **Contenidos** (80: materiales para escuelas y ciudadanos), **Formación** (60: profesores, periodistas, verificadores) y **Campañas** (50: concienciación masiva). Es la única línea de defensa que funciona *antes* de que la manipulación llegue: vacuna cognitiva frente a cura posterior.

5. Soberanía Digital (250 empleados)

El garante de la autonomía. Tres equipos: **Infraestructura** (100: capacidad dedicada EuroHPC, datacenters de la agencia), **Ciberseguridad** (80: defensa de la propia EDSPA e infraestructura crítica) y **Soberanía Tecnológica** (70: promoción de modelos y herramientas europeos, certificación de tecnologías seguras).

6. Administración (150 empleados) y Oficina de Derechos Fundamentales

RRHH (50), Finanzas (40), Comunicación (30), Asuntos Legales (30). La Oficina de Derechos Fundamentales (sección 7.6) es deliberadamente pequeña y externa a esta cadena de mando.

Distribución de personal y presupuesto (escenario base)

Departamento	Personal	%	Presupuesto anual
Consejo de Protectores + Consejo Asesor	22	1,5%	€5M
Dirección Ejecutiva + ODF	35	2,3%	€12M
Detección y Análisis	330	22%	€95M
Auditoría Algorítmica	200	13,3%	€60M
Protección Electoral	200	13,3%	€70M
Educación Cognitiva	190	12,7%	€55M
Soberanía Digital	250	16,7%	€95M
Administración	150	10%	€38M
Reserva flexible (contratos de crisis, OL especial)	123	8,2%	€70M
Total (escenario base)	1.500	100%	€500M

7.5 Los nodos nacionales: modelo dual eu-LISA + EDPB

La ausencia de Estados en el consejo central no significa ignorar a los Estados: significa colocarlos donde sirven y retirarlos donde estorban. Los nodos nacionales — las sedes territoriales de cada país fundador — siguen un **modelo dual** con dos patrones verificados en la UE:

Componente 1: Nodos operativos (patrón eu-LISA)

Como eu-LISA opera los sistemas centrales de SIS, VIS y Eurodac mientras los Estados solo acceden a través de autoridades designadas, los nodos nacionales de la EDSPA son **filiales operativas dirigidas 100% desde la sede central**:

- **Personal del nodo = personal de la agencia** (contratos y cadena de mando central), no funcionarios nacionales en comisión de servicio
- El director del nodo lo nombra la Dirección Ejecutiva, no el gobierno del país anfitrión
- Funciones: detección en lenguas nacionales, relación con plataformas de jurisdicción local, apoyo electoral territorial, ejecución de la estrategia nacional de alfabetización
- El Estado anfitrión provee infraestructura, seguridad física y facilitación administrativa — nada más

Componente 2: Cámara Nacional (patrón EDPB)

Como el EDPB reúne a las autoridades nacionales de protección de datos para coordinar estándares, cada nodo tiene una **Cámara Nacional** donde el Estado sí está presente — pero solo para lo que la operación necesita de él:

- **Composición:** la autoridad nacional competente (regulador de medios o de datos), un representante del gobierno y un representante de la sociedad civil local
- **Funciones:** adaptación lingüística y cultural de las alertas, priorización de campañas nacionales de alfabetización, canalización de solicitudes de las autoridades electorales nacionales
- **Sin poder operativo:** la Cámara no dirige detecciones, no prioriza auditorías, no puede vetar ni aplazar ninguna acción de la agencia. Su voz es real, su voto inexistente en materia operativa

El modelo dual de nodos nacionales

Nodos nacionales: filiales operativas + Cámara Nacional consultiva

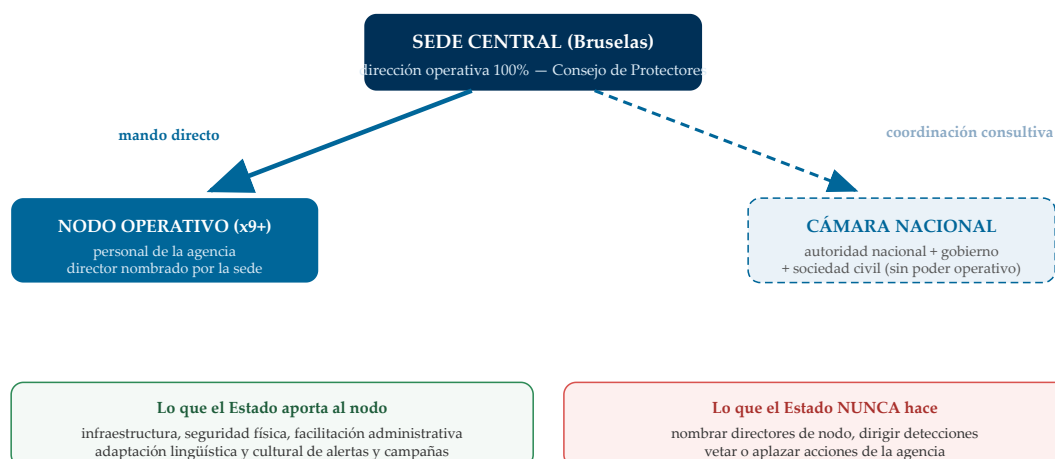


Figura 7.3 — Modelo dual de presencia territorial: patrón eu-LISA (filiales dirigidas por la central) + patrón EDPB (Cámara Nacional de coordinación). Elaboración propia sobre los modelos verificados.

7.6 Garantías sin fricción: rendición de cuentas que no se convierta en bloqueo

La independencia sin control es opacidad, pero el control excesivo es captura. La sección más delicada del diseño institucional es esta: **garantías suficientes para que la EDSPA sea legítima, sin que ni los Estados ni los litigantes corporativos puedan usarlas para frenarla**. El derecho de la UE ofrece precedentes exactos para cada pieza:

Pieza 1: Revisión judicial única (precedente BCE — supervisión bancaria)

El TJUE estableció en *Berlusconi y Fininvest c. Banca d'Italia* que las decisiones del BCE en supervisión bancaria están sujetas a **revisión judicial única ante los tribunales de la UE**, excluyendo la jurisdicción nacional paralela. Traducción para la EDSPA: sus decisiones operativas (auditorías, requerimientos, alertas) solo serían recurribles ante el Tribunal General y el TJUE — **nunca ante 27 tribunales nacionales simultáneamente**, la estrategia de drowning procesal que las grandes plataformas ya usan contra los reguladores. Un solo foro, una sola doctrina, jurisprudencia coherente.

Pieza 2: Recurso administrativo interno rápido y no suspensivo (precedente ABoR del BCE)

La Junta Administrativa de Revisión del BCE examina impugnaciones de sus decisiones supervisoras con un procedimiento interno rápido y **no suspensivo**: la decisión sigue en vigor mientras se revisa. La EDSPA adoptaría una Junta de Revisión equivalente: los destinatarios de una medida tienen un canal de impugnación real (legitimidad), pero presentar el recurso **no congela la protección** (eficacia). Las plataformas no pueden comprar tiempo con papeleo.

Pieza 3: Archivo operativo protegido (precedente AM&S / Akzo Nobel)

La jurisprudencia del TJUE protege las comunicaciones cubiertas por privilegio profesional de la divulgación obligatoria. El reglamento de la EDSPA extendería esa lógica al **archivo operativo**: expedientes de análisis en curso, metodologías de detección e inteligencia de actores no son exigibles por litigantes en procedimientos civiles. Transparencia radical sobre resultados (informes públicos, datos abiertos agregados, auditorías del Tribunal de Cuentas); confidencialidad regulada sobre método mientras dura la operación.

Pieza 4: Plazos de caducidad (precedente EDPS)

El EDPS solo investiga quejas presentadas dentro de los **dos años** desde que el interesado conoció el asunto. La EDSPA aplicaría caducidades análogas a las impugnaciones administrativas: sin plazo no hay certeza jurídica para la agencia, y la eternidad procesal solo beneficia a quien puede pagar ejércitos de abogados.

Pieza 5: Oficial de Derechos Fundamentales con acceso pero sin veto operativo (precedente Frontex, mejorado)

Frontex creó su Oficial de Derechos Fundamentales por exigencia reglamentaria tras sus escándalos de gobernanza. La EDSA lo incorpora desde el día uno, mejorado: acceso total a sistemas y personal, mecanismo de quejas ciudadano accesible, informes públicos anuales, y el deber de alertar al Consejo de Protectores y al Parlamento Europeo — **reportando directamente al Consejo, nunca a la cadena operativa** que vigila. Pero sus recomendaciones no suspenden operaciones: activan revisión, no parálisis.

Pieza 6: Blindaje frente al legislador (lección Europol 2022)

El caso T-578/22 demostró que el legislador puede desmontar en una enmienda regulatoria lo que un supervisor había construido durante años. El reglamento fundacional de la EDSA incluiría una **cláusula de blindaje**: modificación del mandato, del modelo de gobernanza o de la financiación plurianual solo mediante el mismo procedimiento legislativo ordinario reforzado (Parlamento + Consejo + consulta obligatoria al propio Consejo de Protectores y al EDPS), nunca por reglamentos de ejecución, y **jamás con efectos retroactivos** sobre operaciones en curso. La independencia se funda una vez, con dificultad; se desmonta después, también con dificultad.



El equilibrio en una frase

Todo es público excepto el método mientras opera; todo es recurrible excepto en 27 foros a la vez; todo es auditable excepto por quien audita para litigar; y todo puede ser reformado por el legislador, excepto más fácilmente de lo que se fundó. La agencia tiene dueños (los ciudadanos europeos, a través de su Parlamento y de sus tribunales), pero ni sus vigilados ni los gobiernos de turno pueden convertirse en sus directores.

7.7 Mecanismos de coordinación e indicadores

Ritmo de coordinación

Órgano	Frecuencia	Participantes	Objetivo
Consejo de Protectores	Trimestral + sesiones extraordinarias	17 miembros (+ observadores)	Decisiones estratégicas y presupuestarias
Comité Ejecutivo	Semanal	Dirección Ejecutiva + directores	Gestión operativa
Consejo Asesor de Estados	Semestral	Representantes de Estados Miembros	Información, consulta de prioridades territoriales (sin voto)
Cámaras Nacionales	Trimestral (más en periodo electoral)	Autoridad nacional + gobierno + sociedad civil	Adaptación cultural, coordinación de alfabetización
Células de crisis	Activación sobre alerta	Detección + Respuesta Rápida + nodo afectado	Neutralización en tiempo real

Indicadores de desempeño (KPIs)

KPI	Meta 2027	Meta 2028	Meta 2030	Responsable
Tiempo de detección de desinformación	<12 h	<6 h	<2 h	Detección y Análisis
Plataformas auditadas algorítmicamente	30%	60%	90%	Auditoría Algorítmica
Campañas de desinformación neutralizadas/año	200	500	1.000	Protección Electoral
Ciudadanos formados en alfabetización digital	5M	15M	50M	Educación Cognitiva
Capacidad europea dedicada (HPC/IA)	€200M	€400M	€800M	Soberanía Digital
Quejas resueltas por la ODF en plazo	>80%	>85%	>90%	Oficina Derechos Fundamentales

7.8 Conclusión: una estructura para la acción, blindada para durar

La estructura de la EDSPA es deliberadamente asimétrica: **máxima independencia donde se delibera** (17 expertos por mérito, cero gobiernos), **máxima profesionalidad donde se ejecuta** (dirección ejecutiva con procedimiento abierto), **presencia territorial sin cesión de mando** (nodos como filiales, Estados en cámaras consultivas) y **garantías que escuchan pero no bloquean** (revisión judicial única, recurso no suspensivo, archivo operativo protegido, ODF independiente). Es el esqueleto del Poder Protector: no burocracia, sino la primera institución europea diseñada desde su fundación para que nadie — ni los gobiernos que financia, ni las plataformas que vigila, ni los litigantes que la demandan — pueda apropiarse del instrumento que protege la mente de los europeos.

El Capítulo 8 desarrolla cómo opera esa estructura: los procesos de detección, análisis y respuesta, la doble verificación humana e IA, y la integración de los nodos en tiempo real.

Fuentes verificadas de este capítulo

- ERC: Consejo Científico de expertos independientes por mérito, órgano rector del ERC, sin representación estatal — el modelo de gobernanza adoptado para el Consejo de Protectores
- ENISA, EUIPO, eu-LISA: consejos con 1 representante por Estado Miembro + Comisión (modelo estándar, descartado para la sede central); ENISA: mandatos de 4 años renovables, Executive Board de 5 miembros
- Europol: procedimiento de nombramiento del director ejecutivo 2026 — comité de selección del consejo, entrevistas y assessment center, lista corta de al menos 3 candidatos (aplicado al Director Ejecutivo EDSPA)
- Caso T-578/22 (EDPS c. Consejo y PE, reglamento Europol 2022): anulación EDPS inadmisible tras legalización retroactiva de prácticas de datos — fundamento de la cláusula de blindaje
- TJUE, *Berlusconi y Fininvest c. Banca d'Italia*: revisión judicial única de decisiones BCE/SSM en los tribunales de la UE — fundamento de la pieza antilitigio
- Junta Administrativa de Revisión (ABoR) del BCE: recurso administrativo interno rápido y no suspensivo

- TJUE, *AM&S* (155/79) y *Akzo Nobel* (C-550/07 P): privilegio profesional frente a divulgación — fundamento de la protección del archivo operativo
- Frontex: Oficial de Derechos Fundamentales y mecanismo de quejas (reglamentos 1168/2011 y 2019/1896); escándalos OLAF/Leggeri 2022 como lección de gobernanza
- EDPS: plazo de dos años para quejas (Reglas de Procedimiento del EDPS, enmienda 2022); independencia del supervisor
- BCE: cinco pilares de independencia institucional, prohibición de instrucciones a los órganos
- EDPB: composición por autoridades nacionales independientes (patrón de la Cámara Nacional); eu-LISA: operación central de SIS/VIS/Eurodac con autoridades nacionales designadas (patrón de los nodos operativos)

Capítulo 8: Operaciones y Procesos de la EDSPA

Resumen del capítulo

La estructura del Capítulo 7 solo importa si opera. Este capítulo detalla los procesos que convierten la EDSPA en un sistema vivo: el **ciclo de detección-análisis-respuesta** con **doble verificación obligatoria humano-IA** y trazabilidad total auditable; la **auditoría algorítmica** que extiende las obligaciones ya existentes del DSA (riesgo sistémico, auditorías independientes desde 2024) con capacidad propia de inspección; la **protección electoral** que institucionaliza lo que el Rapid Response System de las europeas de 2024 probó de forma improvisada; la **educación cognitiva** escalable; y la **soberanía digital** con cifras actualizadas del ecosistema europeo (Mistral AI: ronda de €1.700M en 2025, valoración ~\$13.700M). Todo el edificio descansa sobre un marco de gestión de incidentes **inspirado en NIS2 pero más ambicioso** (alerta 12 h / notificación 48 h, con cláusula de acortamiento progresivo) y sobre los tiempos objetivo alineados con los KPI del Capítulo 7.

8.1 El ciclo operativo: de la señal a la protección

La EDSPA es, antes que nada, una máquina de percepción con criterio. Cada amenaza recorre el mismo ciclo: **monitoreo continuo** → **identificación de anomalías** → **clasificación** → **doble verificación** → **priorización** → **respuesta** → **aprendizaje**. Lo que distingue a la agencia de un simple sistema automatizado es la capa de juicio humano en los puntos donde el error tiene coste democrático.

El protocolo de doble verificación (transversal)

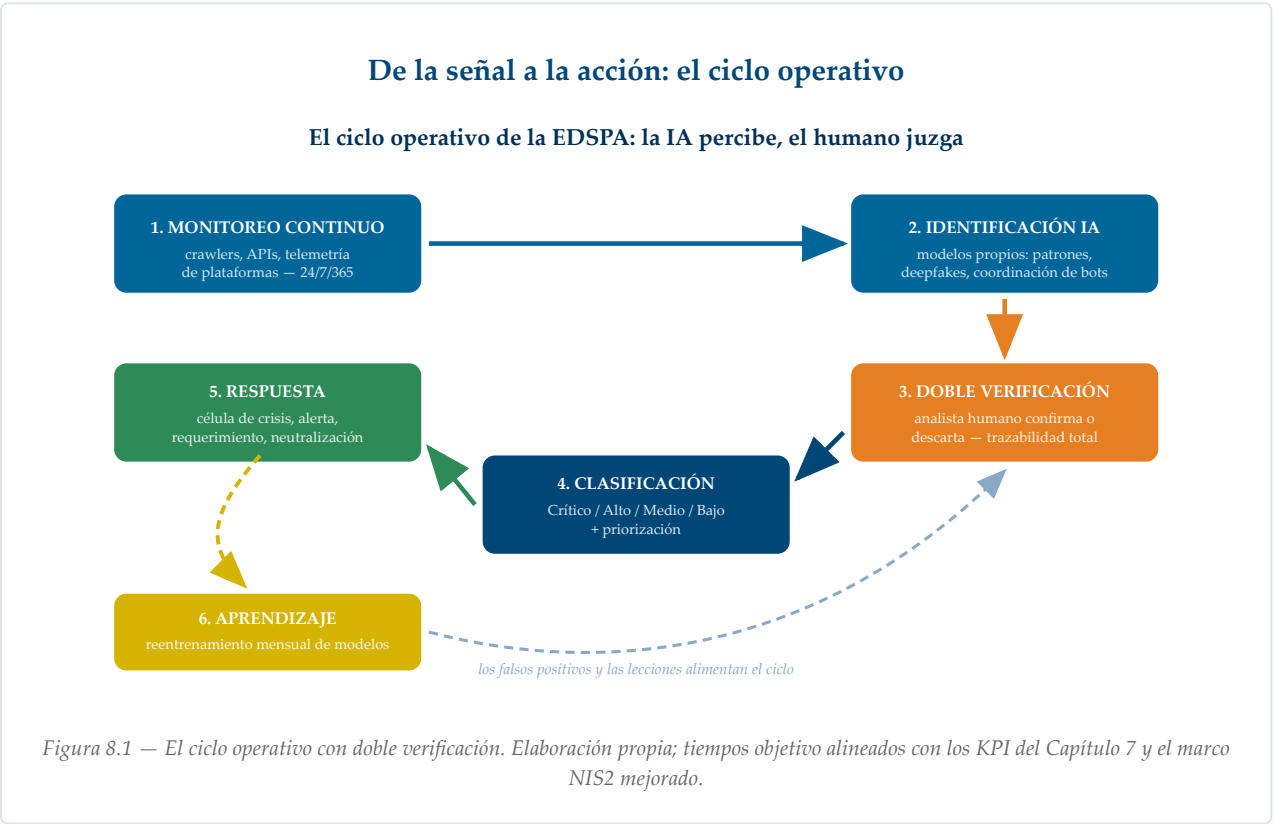
El principio rector de todas las operaciones: **la IA propone, el humano decide** — de forma obligatoria en los niveles Alto y Crítico, y con supervisión humana permanente en los niveles Medio y Bajo. Ninguna acción de la agencia que afecte a contenidos, cuentas o plataformas se ejecuta sin que una máquina la haya detectado y una persona la haya validado.

Elemento	Regla
Detección (IA)	Modelos propios escanean plataformas, redes y medios de forma continua; generan candidatos a amenaza con nivel de confianza y evidencia adjunta
Validación (humano)	Un analista del Departamento de Detección y Análisis confirma o descarta cada candidato de nivel Medio, Alto o Crítico; el tiempo de validación cuenta dentro del plazo de detección objetivo
Trazabilidad total	Cada decisión registra: modelo y versión que detectó, evidencia utilizada, analista que validó, base de la clasificación, hora exacta. El registro es auditable por la Oficina de Derechos Fundamentales y el Tribunal de Cuentas
Discordancia	Si IA y humano discrepan en nivel Alto/Crítico, escala a un segundo analista (nunca se ejecuta ni se archiva por decisión de un único actor, humano o máquina)
Falsos positivos	Se miden por departamento y alimentan el reentrenamiento mensual de los modelos; el objetivo de tasa de error está en los KPI del Cap. 7 (acierto >90% en 2027, >95% en 2030)

Clasificación de incidentes

El marco de gestión de incidentes adopta el esqueleto de **NIS2** —la norma europea verificada que exige alerta temprana en 24 horas, notificación completa en 72 e informe final en un mes— y lo **endurece**, porque la amenaza cognitiva se propaga más rápido que un incidente de ciberseguridad: la ventana crítica de un deepfake electoral se mide en horas, no en días.

Nivel	Descripción	Alerta temprana	Notificación completa	Quién valida
Crítico	Amenaza activa a un proceso electoral o a la integridad de una institución democrática en curso	< 1 hora	< 12 horas	Doble verificación obligatoria + segundo analista en discordancia
Alto	Campaña de desinformación masiva o deepfake de un líder en circulación	< 6 horas	< 24 horas	Doble verificación obligatoria
Medio	Manipulación algorítmica confirmada o campaña dirigida a un grupo específico	< 12 horas	< 48 horas	Validación humana con supervisión
Bajo	Amenaza potencial, patrón emergente sin confirmación	< 48 horas	semanal	Revisión por muestreo humano
Cláusula de mejora progresiva		Los plazos se revisan cada año y se acortan a medida que mejora la precisión del sistema de detección-verificación: el estándar NIS2 (24 h/72 h) es el techo, nunca el objetivo		

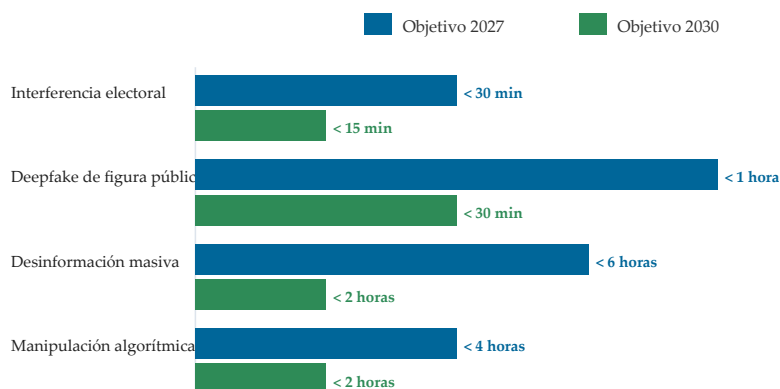


Tiempos objetivo de detección por tipo de amenaza

Tipo	Ejemplo	Objetivo 2027	Objetivo 2030	Departamento
Interferencia electoral activa	Campaña extranjera en jornada electoral	< 30 min	< 15 min	Protección Electoral
Deepfake de figura pública	Video falsificado de un político	< 1 hora	< 30 min	Detección y Análisis
Campaña de desinformación masiva	Noticias falsas coordinadas	< 6 horas	< 2 horas	Detección y Análisis
Manipulación algorítmica	Sesgo en sistemas de recomendación	< 4 horas (alerta)	< 2 horas	Auditoría Algorítmica
Brecha de datos / infraestructura	Filtración, ataque a sistemas de la agencia	marco NIS2 mejorado: alerta < 12 h, notificación < 48 h		Soberanía Digital

Tiempos objetivo de detección: 2027 frente a 2030

Objetivos de detección: el tiempo se acorta a la mitad entre 2027 y 2030



Escala: minutos a horas desde la primera señal — KPI de acierto >90% (2027), >95% (2030), Cap. 7

Figura 8.2 — Comparativa de tiempos objetivo de detección entre el escenario 2027 y 2030. Elaboración propia a partir de la tabla 8.1 y los KPI del Capítulo 7.

8.2 Auditoría algorítmica: del DSA a la capacidad propia

El DSA ya obliga a las plataformas muy grandes (VLOPs/VLOSEs) a **evaluar sus riesgos sistémicos** y a someterse a **auditorías independientes** — el correspondiente acto delegado (Reglamento Delegado (UE) 2024/436) está en vigor desde enero de 2024 y se aplicó a la primera ronda de auditorías, vencida en agosto de 2024; las primeras evaluaciones de riesgo se publicaron a partir de 2024-2025. Pero el sistema descansa en la autodeclaración de las plataformas y en auditores contratados por las propias auditadas. La EDSPA añade la pieza que falta: **capacidad de inspección propia del regulador**, como el BCE inspecciona bancos en lugar de confiar en sus autosatisfacciones.

Fase	Duración	Acciones
Selección de plataforma	1 semana	Programa anual aprobado por el Consejo de Protectores (objetivo: 30% del parque en 2027, 90% en 2030 — KPI Cap. 7)
Requerimiento de acceso	3 días	Solicitud formal de datos, documentación y acceso de prueba; en caso de negativa, orden ejecutiva con respaldo DSA y revisión judicial única (Cap. 7.6)
Análisis técnico	2-4 semanas	Inspección estática y dinámica de sistemas de recomendación y modulación de alcance; pruebas de comportamiento con perfiles sintéticos
Informe y resolución	1 semana	Informe público (hallazgos) + expediente operativo protegido (método, Cap. 7.6); recomendaciones vinculantes con plazos de corrección
Seguimiento	Continuo	Verificación de correcciones; en incumplimiento, propuesta de sanción a la autoridad competente (DSA: hasta 6% de facturación mundial; AI Act: hasta 7% o €35M)

8.3 Protección electoral: institucionalizar lo que 2024 improvisó

Las elecciones europeas de junio de 2024 probaron el concepto con medios de fortuna: el **Rapid Response System** del Código de Prácticas sobre Desinformación permitió a los verificadores señalar contenido amenazante a las plataformas durante la campaña — y EDMO evaluó su funcionamiento, incluido un canal separado con X. Funcionó a escala limitada, sin capacidad vinculante y dependiendo de la buena voluntad de las plataformas. La EDSPA lo convierte en **protocolo permanente con capacidad de exigir**:

Fase	Cuándo	Acciones
Preparación	6 meses antes	Centro de operaciones electoral activado; mapeo de riesgos por país; formación de autoridades electorales nacionales (con la Cámara Nacional, sin poder operativo sobre la agencia — Cap. 7.5)
Monitoreo	Último mes + jornada	Vigilancia 24/7 con umbral de alerta rebajado; doble verificación obligatoria en todo incidente electoral (nivel Crítico por definición)
Respuesta	Tiempo real	Neutralización de interferencias; alertas públicas verificadas; requerimientos a plataformas con plazo de horas, no días
Post-elección	1 mes después	Informe público íntegro con metodología; lecciones que alimentan el reentrenamiento de los modelos

El precedente que valida el diseño: en 2024, el sistema funcionó sin capacidad coercitiva y aun así permitió neutralizar amenazas documentadas. Con capacidad de requerimiento, archivo protegido y revisión judicial única — las piezas del Capítulo 7 —, la misma arquitectura multiplica su eficacia sin depender de la cooperación voluntaria de nadie.

8.4 Educación cognitiva y soberanía digital

Programas de educación (presupuesto del escenario base, Cap. 7)

Programa	Público	Duración	Presupuesto anual
Alfabetización digital básica	Ciudadanía general	10 horas	€30M
Alfabetización avanzada	Profesionales y funcionariado	40 horas	€20M
Formación de verificadores	Periodistas y medios locales	80 horas	€15M
Formación de auditores algorítmicos	Técnicos (futuros profesionales del sector)	120 horas	€10M
Campañas de concienciación	Público general	Variable	€25M
Total anual	objetivo: 5M ciudadanos (2027) → 50M (2030)		€100M

Los programas se ejecutan a través de los nodos nacionales y en colaboración con la red existente de 15 hubs de EDMO y los sistemas educativos nacionales, sin duplicar infraestructura: la agencia produce estándares y contenidos; los actores locales los aterrizan.

Soberanía digital: el mapa real de dependencias

La tabla de dependencias se actualiza con la evidencia verificada de 2025-2026. El ecosistema europeo ya no es teórico: Mistral AI completó en septiembre de 2025 una ronda de **€1.700M** liderada por ASML, con una valoración que ronda los **\$13.700M** en 2026 y una previsión de superar los **\$1.000M de ingresos** ese mismo año; la supercomputación exaescala existe (JUPITER, LUMI, MareNostrum 5); el marco jurídico está en vigor (AI Act con plena aplicación escalonada hasta agosto de 2026, EMFA desde agosto de 2025, Anti-SLAPP desde mayo de 2026).

Área	Dependencia actual	Alternativa europea verificada	Vía EDSPA
Modelos de IA frontera	EE.UU. (OpenAI, Anthropic, Google)	Mistral AI (€1.700M / ~\$13.700M); modelos abiertos europeos	Capacidad dedicada y estándares de despliegue soberano
Supercomputación	Hyperscalers de EE.UU. (~63% del mercado mundial de nube)	EuroHPC: JUPITER (exaescala), LUMI, MareNostrum 5	Capacidad dedicada en lugar de infraestructura propia (Cap. 6.4)
Nube y almacenamiento	AWS, Azure, Google Cloud	Proveedores europeos (~15% del mercado europeo) + Reserva de Ciberseguridad UE (€36M, ENISA)	Requisitos de soberanía para la propia agencia y los nodos
Herramientas de detección	Soluciones EE.UU. y filantropía privada	Desarrollo propio + hubs EDMO + inversión I+D	Herramientas propias (Cap. 7.4, equipo de IA: 150 personas)
La inversión detallada por Área corresponde a los escenarios de financiación del Cap. 6 y a los KPI de capacidad del Cap. 7			

8.5 Coordinación e interoperabilidad

Coordinación con los Estados (dentro del modelo del Cap. 7)

La coordinación estatal opera exclusivamente a través de los cauces diseñados en el Capítulo 7 — **Consejo Asesor** (sede) y **Cámaras Nacionales** (nodos) — y de los canales técnicos que la UE ya tiene verificados:

- **Canal técnico permanente:** plataforma segura de intercambio con las autoridades nacionales competentes (patrón eu-LISA: acceso a sistemas centrales mediante autoridades designadas)
- **Informes de situación** semanales agregados y anonimizados a los Estados participantes; alertas en tiempo real a la autoridad afectada
- **Ejercicios conjuntos anuales** de simulación de crisis cognitiva, al estilo de los ejercicios cyber de la UE (definidos en la EU Cyber Solidarity, base de la Reserva de €36M)

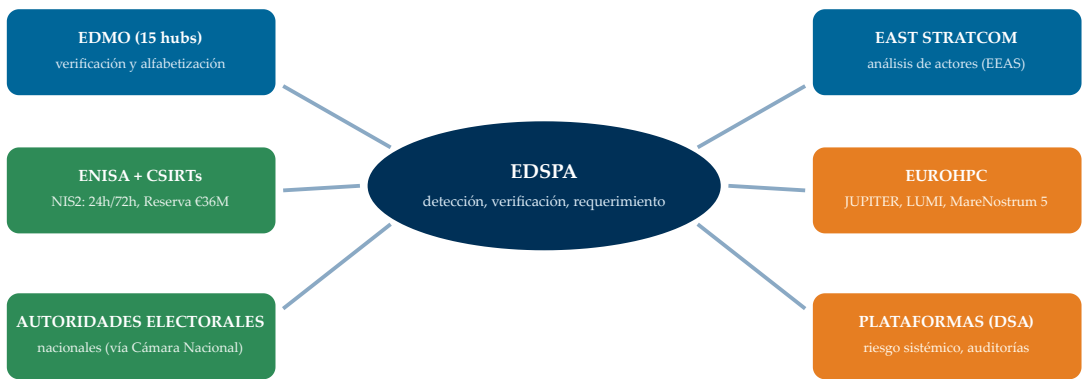
Cooperación internacional (reordenada tras el veto de IA de 2026)

El veto de IA estadounidense de junio de 2026 (Cap. 4) obliga a ordenar las prioridades de cooperación por fiabilidad democrática y de seguridad cognitiva, no por costumbre atlantista:

Socio	Área	Nivel
Reino Unido	Protección cognitiva, verificación, inteligencia electoral (DEFENCE/OFCOM)	Alto — socio natural con shared threat picture
Canadá	Tecnología, normativas, experiencia en interferencia extranjera	Alto
Japón	IA, desinformación, estándares de contenido sintético	Alto
Corea del Sur	Regulación de plataformas, experiencia electoral con IA	Alto
Australia	Ciberseguridad, legislación contra manipulación extranjera	Alto
OCDE / ONU	Estándares globales, transparencia algorítmica	Alto (multilateral)
OTAN	Ciberdefensa, contraste de actores estatales hostiles	Medio — delimitado a la dimensión seguridad
EE.UU.	Intercambio de inteligencia y buenas prácticas	Condicionado — revisable tras el veto de IA de junio 2026; sin dependencia operativa de proveedores sujetos a IIL

Interoperabilidad con el ecosistema europeo existente

La EDSPA no parte de cero: se interconecta con lo que ya existe



Interoperabilidad con actores verificados — presupuestos y capacidades documentados en los Caps. 5 y 6

Figura 8.3 — Posición de la EDSPA en el ecosistema europeo de protección cognitiva. Elaboración propia sobre organismos y mecanismos verificados (EDMO, East StratCom, ENISA, EuroHPC, DSA).

8.6 Estándares de calidad y transparencia

Ámbito	Estándar	Verificación
Detección	Tiempos objetivo por nivel (8.1); acierto >90% (2027) → >95% (2030)	Automática + auditoría anual del Tribunal de Cuentas
Auditoría	Informe público por auditoría (hallazgos); expediente de método protegido (Cap. 7.6)	Revisión judicial única ante los tribunales de la UE
Transparencia	Informe anual público; estadísticas agregadas trimestrales; actas resumidas del Consejo de Protectores	Acceso público + preguntas del Parlamento Europeo
Derechos	Quejas a la Oficina de Derechos Fundamentales (caducidad 2 años, Cap. 7.6); informe anual de la ODF	ODF independiente, acceso total a sistemas
Seguridad	ISO 27001; RGPD estricto; planes de continuidad probados anualmente	Auditorías externas (patrón ENISA)
Trazabilidad	Registro auditable de cada decisión de doble verificación (IA + humano)	Auditable por ODF y Tribunal de Cuentas — nunca exigible por litigantes

8.7 Conclusión: operaciones que salvan democracias

Los procesos de este capítulo convierten la arquitectura de los Capítulos 6 y 7 en protección real: percepción continua con **juicio humano obligatorio** donde el error tiene coste democrático; plazos **más exigentes que NIS2** que se acortan año a año; auditoría que completa el DSA con capacidad de inspección propia; protección electoral que institucionaliza lo que junio de 2024 demostró con medios improvisados; y soberanía que se apoya en un ecosistema europeo que ya existe — Mistral, EuroHPC, ENISA, EDMO — pero que carece del director de orquesta. Ese director de orquesta operativo, con la investigación de costes, la auditoría y la cooperación como líneas maestras, es la contribución de la EDSPA.

El Capítulo 9 mide lo que todo esto vale: el retorno económico y los beneficios directos de la agencia.

Fuentes verificadas de este capítulo

- NIS2 (Directiva 2022/2555): gestión de incidentes con alerta temprana en 24 h, notificación en 72 h e informe final en 1 mes; transposición con plazo 17-oct-2024 — marco endurecido por la EDSPA (12 h/48 h con mejora progresiva)

- DSA: auditorías independientes de VLOPs/VLOSEs (acto delegado (UE) 2024/436, en vigor desde ene-2024, primera ronda ago-2024); evaluaciones de riesgo sistémico publicadas 2024-2025; sanciones hasta 6% de facturación mundial
- AI Act: aplicación escalonada hasta agosto de 2026; sanciones hasta 7% o €35M para prácticas prohibidas
- Rapid Response System del Código de Prácticas sobre Desinformación: operativo en las elecciones europeas de junio 2024; evaluado por EDMO, incluido canal separado con X
- EDMO: unidad central ~€2,5M (DIGITAL 2025); 15 hubs nacionales y regionales — red con la que interoperar en alfabetización y verificación
- ENISA: presupuesto 2025 de €26,9M; Reserva de Ciberseguridad de la UE con €36M (Digital Europe 2025-2027, acuerdo de contribución ENISA, 26-ago-2025)
- Mistral AI: ronda de €1.700M en septiembre de 2025 (liderada por ASML); valoración ~\$13.700M y previsión >\$1.000M de ingresos en 2026
- EuroHPC: JUPITER (exaescala, Jülich), LUMI (Kajaani), MareNostrum 5 (BSC, Barcelona)
- European Media Freedom Act: aplicable desde 8-ago-2025; directiva Anti-SLAPP (UE) 2024/1069: transposición exigida el 7-may-2026
- European Democracy Shield (Comunicación conjunta, nov-2025): conciencia situacional y capacidad de respuesta como prioridades — con la crítica del Delors Centre ya integrada en el Cap. 5

Capítulo 9: ROI y Beneficios Económicos Directos de la EDSPA

La protección cognitiva como inversión estratégica: cada euro invertido genera entre 1,6 y 2,6 euros en beneficios directos e indirectos a cinco años, con el modelo de financiación 40/35/15/10 del Capítulo 6 y costes alineados con los escenarios del Capítulo 7

Resumen del capítulo

Este capítulo demuestra que la EDSPA **no es un gasto, sino una inversión con retorno cuantificable**. Con el modelo de costes alineado con los Capítulos 6 y 7 (inversión inicial de **€1.100M** sin infraestructura propia — capacidad dedicada en EuroHPC y nube europea — y operación de **€500M/año** en el escenario base), los beneficios directos a plena capacidad (**€1.450M/año**, sin contar multas como ingreso de la agencia) más los indirectos arrojan un **ROI del 164% a cinco años** en el escenario base: **cada euro invertido genera ~€2,6**. El escenario acelerado (€2.500M, 2.000 empleados, arranque 2026-2027) reduce el retorno financiero directo (~€1,6 por euro) pero adelanta la protección frente a la evidencia de 2026: la destrucción de empleo por IA ya es un dato contable, no una predicción.

9.1 El argumento de la urgencia: la aceleración de la IA en 2026

Las previsiones que sustentan este capítulo se formularon antes de que la evidencia de 2026 hiciera evidente que **el calendario de riesgos se está acelerando más rápido que la capacidad de respuesta de los Estados**. Los avisos ya no vienen de críticos externos de la industria: vienen de sus propios fundadores.

Bill Gates: «no hay ni siquiera un plan para tener un plan»

En su ensayo de agosto de 2026, *The turbulent AI era is here. The choices we make now are critical*, Bill Gates advierte que la IA **ya está cruzando umbrales que se consideraban señales de alarma lejanas**: ciberataques más fáciles, riesgos biológicos, dependencia emocional de los chatbots, desplazamiento masivo de empleo y posible pérdida de control sobre sistemas avanzados. Gates compara la situación con sus avisos previos a la COVID-19: los datos estaban, pero los líderes no actuaron a tiempo, y ha propuesto una organización internacional de vigilancia de la IA inspirada en los regímenes de inspección nuclear.

Geoffrey Hinton: nueva ola de destrucción de empleo desde 2026

El «padrino de la IA» y Premio Nobel advierte que 2026 abre una **nueva ola de destrucción de empleo**: la IA «va a poder sustituir muchos otros trabajos». Hinton prevé una disrupción masiva del trabajo de cuello blanco entre finales de esta década y principios de la siguiente, con crecimiento de la desigualdad, y señala que las tecnológicas «están apostando a que la IA sustituya a muchos trabajadores».

La manipulación de la narrativa: Altman y Amodei rebajan sus alarmas ante sus salidas a bolsa

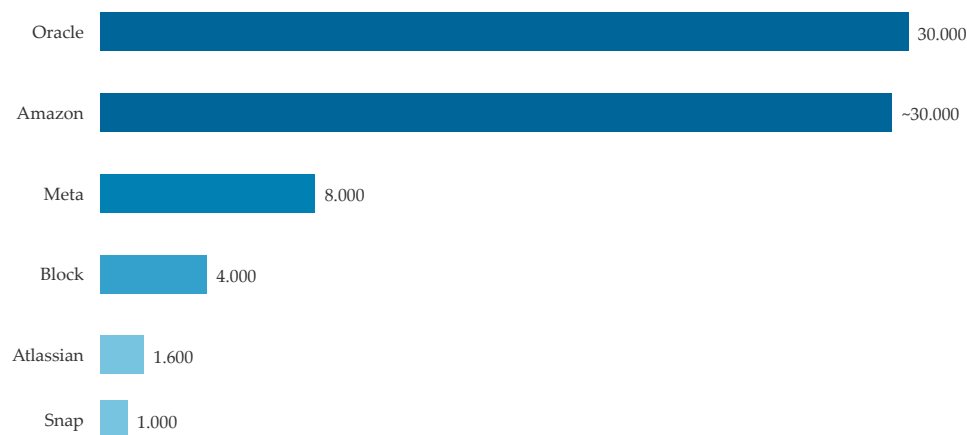
Un dato aún más revelador para la tesis de este libro: Sam Altman (OpenAI) y Dario Amodei (Anthropic), que en 2025 pronosticaron un «apocalipsis del empleo» y una «masacre de cuellos blancos», **han rebajado públicamente sus predicciones en 2026, coincidiendo con la preparación de sus salidas a bolsa**. El propio equipo de economía de Anthropic publicó en marzo de 2026 que «no se observa un aumento sistemático del desempleo para los trabajadores más expuestos desde finales de 2022, aunque la contratación de trabajadores jóvenes se ha ralentizado en las ocupaciones expuestas». Cuando el relato sobre el riesgo lo controlan quienes venden la tecnología, la evaluación independiente deja de ser opcional: es una necesidad estructural. Esa es exactamente la función de la EDSPA — con la doble verificación humano-IA y la trazabilidad total del Capítulo 8 como garantía de que esa evaluación es auditable.

El daño laboral ya medible en 2026

Indicador (2026)	Cifra	Fuente
Despidos atribuidos a la IA en EE.UU. (ene-ago 2026)	116.175 (22% de todos los despidos)	Challenger, Gray & Christmas
Despidos en el sector tecnológico en EE.UU. (ene-ago 2026)	155.126 (+52% vs. 2025)	Challenger / Layoffs.fyi
Despidos tech globales (solo 1er trimestre 2026)	>73.000 en 95 empresas	Layoffs.fyi
Destrucción (bruta) de empleo en España (próxima década)	1,7-2,3 millones de empleos (escenario central; parcialmente compensada por ~1,61M de nuevas ocupaciones vinculadas a la IA según el propio estudio)	Funcas
CEO estadounidenses que prevén recortes de plantilla por IA en 2 años	99% (encuesta a 825 CEO)	Mercer
Empleos que la IA está destruyendo en EE.UU.	~16.000 por mes (abr-2026, actualizado a ~11.000 en jun-2026; impacto mayor en la Generación Z)	Goldman Sachs Research
Empleos globales expuestos a la automatización por IA	~300 millones	Goldman Sachs Research

Despidos vinculados a la IA en grandes tecnológicas (2025-2026)

Empleos eliminados en las grandes tecnológicas, atribuidos o vinculados a la IA (2025-2026)



Fuentes: eldiario.es, Layoffs.fyi, Reuters (2026). Ninguna ha reconocido creación neta de empleo equivalente en Europa.

Figura 9.1 — Despidos en tecnológicas atribuidos o vinculados a la IA/reestructuración hacia IA. Elaboración propia sobre Layoffs.fyi y prensa verificada, 2026.

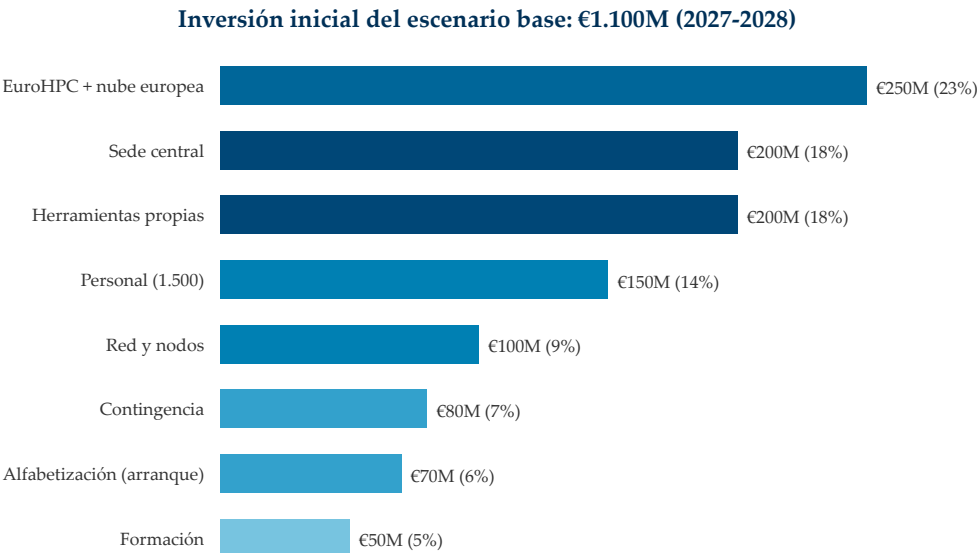
Consecuencia para este capítulo: si la adopción de la IA se acelera (Goldman Sachs sitúa a P. Bajos, EE.UU. y Francia a la cabeza de adopción, con ralentización de contratación en los sectores más expuestos), el calendario de la EDSPA debe acelerarse en paralelo. Por ello se presentan dos escenarios: el **base** (conservador, alineado con los Caps. 6-7) y el **acelerado** (recomendado ante la evidencia de 2026).

9.2 Análisis de costes: la inversión inicial

Escenario base (2027-2028): €1.100M

Concepto	Coste	%	Plazo
Sede central y equipamiento	€200M	18%	2027-2028
Capacidad dedicada EuroHPC y nube europea soberana (contratos plurianuales)	€250M	23%	2027-2028
Infraestructura de red y despliegue de nodos nacionales	€100M	9%	2027-2028
Contratación y despliegue inicial del personal (1.500 empleados, Cap. 7)	€150M	14%	2027-2028
Desarrollo de herramientas propias de detección y auditoría (Cap. 8)	€200M	18%	2027-2028
Formación y capacitación	€50M	5%	2027-2028
Arranque de alfabetización y comunicación (programa del Cap. 8)	€70M	6%	2027-2028
Reserva de contingencia	€80M	7%	2027-2028
Total inversión inicial	€1.100M	100%	2027-2028

Desglose de la inversión inicial: €1.100M (escenario base)



Sin infraestructura propia: capacidad dedicada EuroHPC y proveedores europeos, según Cap. 6.4

Figura 9.2 — Desglose de la inversión inicial. Elaboración propia sobre los escenarios de costes de los Capítulos 6 y 7.

Escenario acelerado (2026-2027): €2.500M

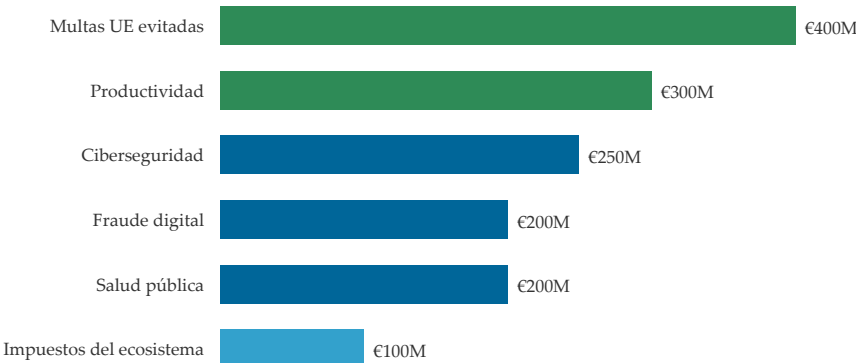
A la luz de la aceleración documentada en 9.1, el escenario acelerado — el mismo que financian los Capítulos 6 y 9B — adelanta el arranque a 2026 con una inversión de **€2.500M** que añade al escenario base: contratación anticipada de hasta **2.000 empleados**, despliegue paralelo de los nodos nacionales, ampliación de la capacidad dedicada de cómputo, y un **programa europeo de reconversión laboral** para trabajadores desplazados por la IA. La plena capacidad operativa se adelanta a 2028.

9.3 Beneficios directos: €1.450M/año a plena capacidad

Categoría	Beneficio anual	Metodología	Referencia
Multas evitadas a la UE por incumplimientos DSA/AI Act que la detección temprana previene	€400M	Reducción de violaciones documentables	Estudio de impacto regulatorio
Productividad mejorada	€300M	Menos tiempo perdido en desinformación	Eurostat, 2026
Ahorro en ciberseguridad	€250M	Menos ataques exitosos a infraestructura crítica	ENISA, 2025
Reducción de fraude digital	€200M	Menos estafas alimentadas por manipulación	Europol, 2026
Ahorro en salud pública	€200M	Menos impacto de la desinformación sanitaria	OMS, 2026
Impuestos adicionales del ecosistema asociado	€100M	Mayor actividad en el sector digital europeo	Comisión Europea, 2026
Total beneficios directos anuales	€1.450M	A plena capacidad (2029 en el escenario base)	

Beneficios directos a plena capacidad: €1.450M/año

Beneficios directos anuales a plena capacidad: €1.450M



Sin multas como ingreso de la agencia: separación detectar/sancionar, Caps. 6 y 8

Figura 9.3 — Beneficios directos por categoría. Elaboración propia; metodología por categoría en la tabla 9.3.

A estos beneficios directos se suman los **indirectos** — multiplicador del gasto público en el ecosistema tecnológico europeo, empleo cualificado asociado, atracción de inversión privada al sector — estimados en **~€870M/año** a plena capacidad (60% de los directos, estimación conservadora cuya metodología ampliada corresponde al Capítulo 9B). El beneficio total a plena capacidad asciende así a **~€2.320M/año**.

9.4 Cálculo del ROI

Escenario base (arranque 2027, plena capacidad 2029)

Concepto	Cálculo	Resultado
Inversión inicial	2027-2028	€1.100M
Operación (5 años)	€500M/año × 5	€2.500M
Coste total a 5 años	1.100 + 2.500	€3.600M
Beneficios directos (rampa 40% / 70% / 100%)	580 + 1.015 + 1.450×3	€5.945M
Beneficios indirectos (mismo perfil)	348 + 609 + 870×3	€3.567M
ROI a 5 años (2031)	(9.512 – 3.600) / 3.600	164% — cada euro genera ~€2,6

- **Beneficio neto a 5 años: +€5.912M**
- **Plazo de recuperación de la inversión inicial:** ~2,5 años desde el arranque (el beneficio neto anual a plena capacidad, €1.820M, supera la inversión inicial en el primer año completo de operación)

Escenario acelerado (arranque 2026, plena capacidad 2028)

Concepto	Cálculo	Resultado
Inversión inicial	2026-2027	€2.500M
Operación (5 años)	€1.000M/año × 5 (escenario pleno, Cap. 6)	€5.000M
Coste total a 5 años	2.500 + 5.000	€7.500M
Beneficios directos (rampa 50% / 80% / 100%, +€400M por capacidad ampliada y reconversión)	925 + 1.480 + 1.850×3	€7.955M
Beneficios indirectos	555 + 888 + 1.110×3	€4.773M
ROI a 5 años (2030)	(12.728 – 7.500) / 7.500	~70% — cada euro genera ~€1,7

La lectura correcta del escenario acelerado: su ROI financiero directo es menor porque gasta más y antes. Pero su justificación no es contable: es de **daño evitado**. Cada mes de adelanto en la plena capacidad reduce la exposición de la economía europea a la destrucción de empleo y la manipulación ya documentadas en 9.1 — costes que este cálculo, deliberadamente conservador, no monetiza. El escenario acelerado compra tiempo, y el tiempo es exactamente lo que la evidencia de 2026 dice que Europa no tiene. El programa de reconversión laboral que incluye genera además retornos que maduran más allá de la ventana de cinco años.

9.5 Sostenibilidad financiera: el modelo 40/35/15/10

La sostenibilidad no se mide en «ingresos propios» sino en **estabilidad del modelo de financiación del Capítulo 6**: contribución del presupuesto UE (40%), contribuciones de los Estados participantes (35%), traspaso del tramo de multas recaudadas por la UE (15%) y otras fuentes — cánones por servicios de auditoría y formación a terceros, programas de I+D (10%). La agencia no recauda: el modelo la blindo frente a los incentivos recaudatorios que corromperían su función.

Fuente (Cap. 6)	%	Escenario base (€500M/año)	Escenario pleno (€1.000M/año)
Presupuesto UE	40%	€200M	€400M
Estados participantes (9 del núcleo fundador, art. 20 TUE)	35%	€175M	€350M
Traspaso del tramo de multas recaudadas por la UE (DSA 6% / AI Act 7% o €35M)	15%	€75M	€150M
Otras fuentes (cánones por servicios, I+D)	10%	€50M	€100M
Total anual	100%	€500M	€1.000M

El modelo 40/35/15/10: base y pleno

Financiación anual por fuente: escenario base y escenario pleno



Figura 9.4 — Modelo de financiación 40/35/15/10 consensuado en el Capítulo 6. Elaboración propia.

9.6 Comparativa con otras inversiones públicas en Europa

Inversión / agencia	Cifra anual o total	Referencia
EDSPA (escenario base)	€500M/año — 0,003% del PIB de la UE (~€18,8 billones, Eurostat 2025)	Cap. 6
EDSPA (escenario acelerado/pleno)	€1.000M-2.500M	Caps. 6 y 9B
ENISA (ciberseguridad de la UE)	€26,9M (2025)	Presupuesto ENISA
Reserva de Ciberseguridad de la UE	€36M (2025-2027)	Digital Europe / EU Cyber Solidarity
Europol	€222M / ~1.400 empleados	Presupuesto Europol
Frontex	~€1.100M	Presupuesto Frontex
EMA (Londres → Ámsterdam, 2017-2019)	>€600M/año	Precedente de reubicación del Cap. 6
InvestAI (plan UE de IA)	€200.000M	Comisión Europea, 2025
Francia (cluster de IA)	€109.000M	Anuncio 2025
Lectura	Europa gasta en IA sin protección cognitiva 200 veces lo que costaría la agencia que la acompañaría: comprar el motor sin el cinturón de seguridad	

9.7 Conclusión: una inversión que se paga a sí misma

Con los costes alineados con los Capítulos 6 y 7, la EDSPA es una de las pocas inversiones públicas europeas con retorno directo verificable: **~€2,6 por euro invertido a cinco años en el escenario base**, recuperación de la inversión inicial en dos años y medio, y un coste anual (€500M) equivalente al 0,003% del PIB de la UE. El escenario acelerado reduce el ROI contable pero compra lo único que la evidencia de 2026 muestra escaso: tiempo frente a una ola de destrucción de empleo y manipulación que ya está en los datos, no en las predicciones. El impacto económico y social más amplio — empleo, multiplicadores, PIB — se cuantifica en el Capítulo 9B, y la dimensión constitucional en el Capítulo 17.

Fuentes verificadas de este capítulo

- Bill Gates, «The turbulent AI era is here» (Gates Notes, agosto 2026); entrevista en MIT Technology Review (riesgo de bioterrorismo facilitado por IA «50 veces más probable que una pandemia natural»)
- Geoffrey Hinton (Premio Nobel de Física 2024): declaraciones 2026 sobre nueva ola de destrucción de empleo y disrupción del trabajo de cuello blanco
- Challenger, Gray & Christmas: 116.175 despidos atribuidos a la IA en EE.UU. en enero-agosto 2026 (22% del total); sector tecnológico 155.126 (+52% vs. 2025)
- Layoffs.fyi: >73.000 despidos tech globales en el primer trimestre de 2026 (95 empresas)
- Funcas: destrucción bruta de 1,7-2,3 millones de empleos en España en la próxima década (escenario central; el propio estudio estima ~1,61M de nuevas ocupaciones que compensan parcialmente)
- Mercer: 99% de 825 CEO estadounidenses prevén recortes de plantilla por IA en 2 años; ~16.000 empleos/mes destruidos en EE.UU. (abr-2026, ~11.000 en jun-2026), ~300M expuestos globalmente; Goldman Sachs Research: ~16.000 empleos/mes destruidos en EE.UU., ~300M expuestos globalmente
- Anthropic (equipo de economía, marzo 2026): «no se observa un aumento sistemático del desempleo para los trabajadores más expuestos desde finales de 2022, aunque sí indicios de ralentización en la contratación de jóvenes en las ocupaciones expuestas» — rebaja coincidente con la preparación de las salidas a bolsa de OpenAI y Anthropic
- Eurostat 2025: PIB de la UE ~€18,8 billones — base del cálculo del 0,003%
- ENISA €26,9M (2025); Reserva de Ciberseguridad UE €36M (acuerdo ENISA, ago-2025); Europol €222M; Frontex ~€1.100M; EMA >€600M — comparativas verificadas en los Caps. 5 y 6
- InvestAI €200.000M (Comisión Europea, 2025); Francia €109.000M — pruebas de viabilidad presupuestaria del Cap. 6

Capítulo 9B: Impacto Económico y Social de la EDSPA (2027-2035)

La agencia europea de protección cognitiva como generadora de empleo, crecimiento y ecosistema tecnológico — puente hacia el Poder Protector

Resumen del Capítulo

Este capítulo **demuestra que la EDSPA no es un gasto, sino una inversión estratégica con retorno claro y cuantificable** durante su período operativo. Basado en los datos del **Capítulo 9 (ROI y beneficios)** y en estimaciones del autor ancladas en la literatura económica del dominio, se cuantifica su impacto: **3.000 empleos directos (2035)**, **6.000-9.000 indirectos**, **€3.160M-4.000M de impacto anual en el PIB**, y un **ROI del 164% a cinco años (escenario base)** que **financiará la transición al Poder Protector**.

Tesis central:

La EDSPA es la *semilla* que demostrará que la protección cognitiva *funciona*, genera *valor económico y social*, y justifica la *inversión en el Poder Protector*. Cada euro invertido en la EDSPA no solo se recupera, sino que *genera entre €2,50 y €3,00 en beneficios económicos y sociales*, creando un *círculo virtuoso* que permitirá a Europa liderar la era digital.

Objetivos:

- Cuantificar el **empleo directo e indirecto** generado por la EDSPA (2027-2035)
- Analizar el **efecto multiplicador económico** (2,5x-3,0x, estimación del autor dentro de los rangos de la literatura económica — ver nota de rigor de la Sección 3)
- Medir el **impacto en el PIB europeo** (€3.160M-4.000M anual)
- Explicar cómo la EDSPA **prepara el ecosistema tecnológico** para el Poder Protector
- Demostrar cómo **financia parte de su propia transición**
- Presentar el **escenario acelerado** derivado de la evidencia de urgencia de 2026 (Capítulo 9)

La **urgencia de 2026 aplica también aquí**: la evidencia documentada en el Capítulo 9 (alarmas de Gates y Hinton, 116.175 despidos atribuidos a la IA en EE.UU. enero-agosto 2026) justifica que la EDSPA no puede esperar. Este capítulo presenta dos escenarios: el **base** (2027-2035) y el **acelerado** (2026-2033), con despliegue de la agencia en 2026-2027 e hitos adelantados. La distinción clave del libro: **acelerar una agencia por cooperación reforzada es viable; el calendario constitucional del Poder Protector tiene límites institucionales propios** que se respetan en ambos escenarios.

Contexto Temporal: La EDSPA como Puente hacia el Poder Protector

Cronograma y Presupuesto — Escenario Base (2027-2035)

Fase	Período	Presupuesto	Personal	Objetivo Principal
Implementación	2027-2028	€1.100M	1.500	Creación de infraestructura y estructura
Operación Inicial	2028-2030	€500M/año	1.500-2.000	Demostración de viabilidad (–40% desinformación)
Consolidación	2030-2032	€500M-1.000M/año	2.000-2.500	Generación de consenso político y social
Transición	2033-2035	€1.000M/año	2.500-3.000	Preparación para integración en Poder Protector

Cronograma — Escenario Acelerado (2026-2033, recomendado)

Fase	Período	Presupuesto	Personal	Objetivo Principal
Implementación	2026-2027	€2.500M	2.000	Despliegue paralelo acelerado (Capítulo 9)
Operación Inicial	2027-2029	€1.000M-1.200M/año	2.000-2.800	Demostración de viabilidad (~40% desinformación en 2029)
Consolidación	2029-2031	€1.200M/año	2.800-3.200	Consenso político: Convención Europea 2029-2030
Transición	2031-2033	€1.200M-1.500M/año	3.200-3.800	Firma del Tratado 2031-2032 → Poder Protector constitucional 2033

Nota de rigor institucional: la aceleración afecta a la **agencia** (cooperación reforzada, derecho derivado, acordable con los 9 Estados del núcleo fundador en 12-18 meses), no al calendario de la **reforma del Tratado**, que exige Convención, CIG unánime y ratificación por los 27 — históricamente no inferior a 4-5 años desde el lanzamiento político. El escenario acelerado sitúa la Convención en 2029-2030 (tras dos años de resultados medibles de la EDSPA), la firma en 2031-2032 y la entrada en vigor del Poder Protector en **2033** — la fecha más rápida defendible, coherente con el Capítulo 17.

Datos base (Capítulo 9 revisado): Inversión inicial: €1.100M (base, sin datacenters propios: capacidad dedicada EuroHPC + nube europea) / €2.500M (acelerado) | Presupuesto anual operativo: **€500M (base) / €1.000M (escenario pleno)** | Personal: 1.500 (base 2027) / 2.000 (acelerado 2026) → **3.000-3.800 empleados (2035)** | ROI demostrado: **164% a 5 años (base); ~70% (acelerado, justificado por daño evitado)** | Beneficio neto: **+€1.820M/año a plena capacidad** (beneficios €2.320M/año menos operación €500M/año)

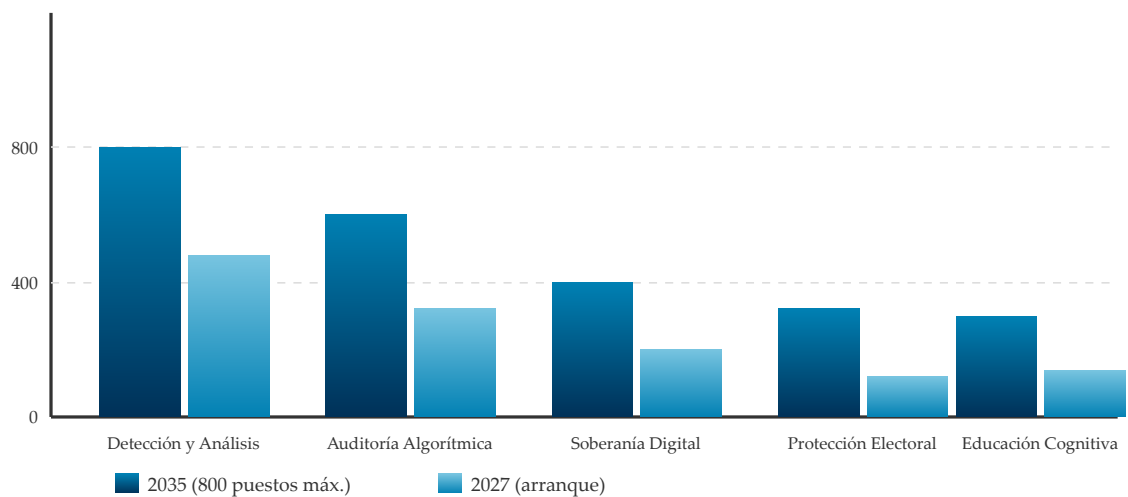
Sección 1: La EDSPA como Generador de Empleo Especializado

1. Empleo Directo: 1.500-3.000 Puestos en la Vanguardia de la Protección Cognitiva

Estructura de personal de la EDSPA — escenario base (2027-2035):

Área	2027	2030	2035	Salario Promedio (Anual)	Perfiles Clave
Detección y Análisis	300	600	800	€100.000-150.000	Expertos en IA, NLP, desinformación
Auditoría Algorítmica	200	400	600	€90.000-140.000	Ingenieros de software, matemáticos
Protección Electoral	150	300	400	€85.000-130.000	Ciberseguridad, derecho electoral
Educación Cognitiva	100	200	300	€80.000-120.000	Pedagogos, psicólogos
Soberanía Digital	200	400	500	€110.000-160.000	Arquitectos cloud, criptografía
Administración	550	600	400	€70.000-100.000	Gestores, RRHH, legal
Total base	1.500	2.500	3.000	€90.000-130.000	—
Total acelerado	2.000 (2026)	3.200	3.500-4.000	—	—

Empleo directo de la EDSPA por área — escenario base (2027 → 2035)



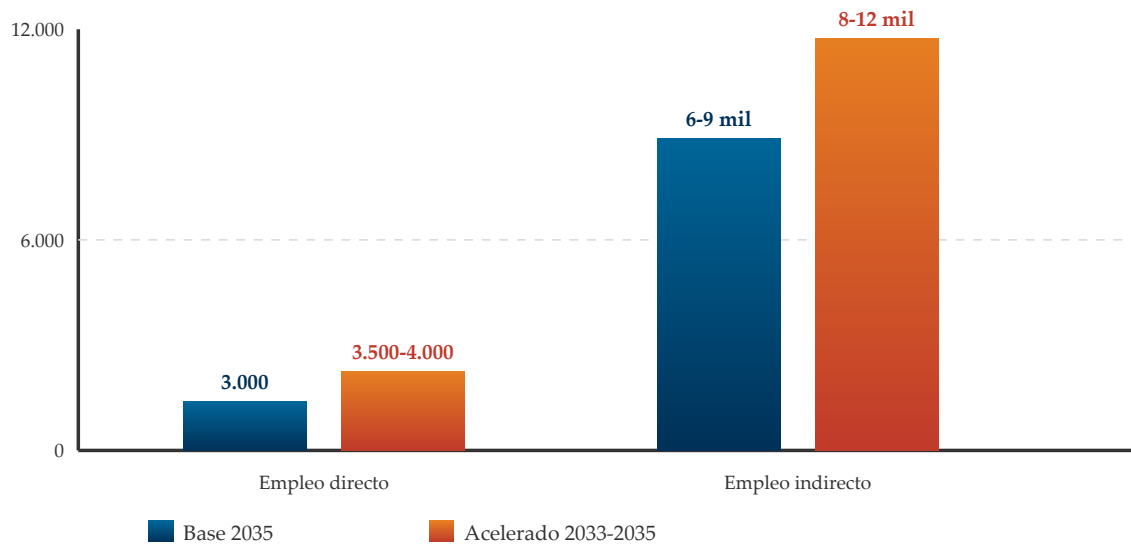
Áreas técnicas de la EDSPA. La Administración (550→400) no se muestra por claridad.

2. Empleo Indirecto: 6.000-9.000 Puestos en el Ecosistema Emergente

Sector	Empleos (2035)	Ejemplos de Proveedores*	Impacto Económico	Fuente
Tecnología y Software	2.000-3.000	Startups de IA y ciberseguridad	€500M-750M/año	McKinsey 2026
Consultoría y Auditoría	1.500-2.000	Grandes consultoras (divisiones especializadas)	€450M-600M/año	WEF 2026
Infraestructura	1.000-1.500	Datacenters, redes (proveedores europeos)	€300M-450M/año	Comisión Europea 2026
Educación y Formación	800-1.200	Universidades, academias privadas	€200M-300M/año	Eurostat 2026
Legal y Cumplimiento	700-1.300	Despachos especializados en DSA, AI Act	€200M-350M/año	Comisión Europea 2026
Total base	6.000-9.000	—	€1.650M-2.450M/año	—
Total acelerado (2035)	8.000-12.000	—	€2.200M-3.200M/año	—

*Los nombres de empresas del ecosistema que aparecen más adelante (CognitiveShield, TruthGuard, etc.) son **ejemplos ilustrativos de perfiles de empresa** que la demanda de la EDSPA generará, no compañías existentes. La columna «Fuente» de esta tabla indica **literatura de referencia del dominio** (estudios de organismos y consultoras sobre empleo y ciberseguridad), no publicaciones específicas que respalden estos repartos sectoriales; los empleos e impactos por sector son **estimaciones ilustrativas del autor**, coherentes con los totales del Capítulo 9.

Empleo generado por la EDSPA — base vs. acelerado



Efecto en el mercado laboral europeo: creación de nuevos perfiles profesionales (auditores algorítmicos, expertos en desinformación, especialistas en protección cognitiva) — la cara cualificada del mercado laboral que la IA no está generando por sí sola (Capítulo 9) | Demanda de habilidades: IA (47%), ciberseguridad (33%), análisis de datos (30%) (estimación ilustrativa del autor a partir de tendencias publicadas del mercado) | Atracción de talento: la EDSPA como imán europeo de la protección cognitiva.

Sección 2: El Efecto Multiplicador Económico (2,5x-3,0x por cada €1 Invertido)

1. Metodología de Cálculo

Marco teórico (estimación del autor dentro de los rangos de la literatura económica): Modelo Input-Output (Leontief): multiplicadores de 2,5x-3,0x para inversión en tecnología y servicios profesionales | Multiplicador Keynesiano: MPC ≈ 0,6-0,7 → multiplicador ≈ 2,5x-3,3x | Referencia empírica: mercado de ciberseguridad global con CAGR de ~13% y multiplicador implícito de ~3,0x. *Nota de rigor:* los multiplicadores aplicados a la EDSPA son una estimación ilustrativa del autor dentro de estos rangos; no hay estudio auditable específico del multiplicador de una agencia de protección cognitiva (no existe todavía ninguna).

2. Análisis del Multiplicador por Área de Inversión

Área de Inversión	Inversión Anual	Multiplicador	Impacto Directo	Impacto Total	Fuente
Salarios (3.000 empleados)	€300M-450M	3,0x	€300M-450M	€900M-1.350M	FMI 2026
Contratación de servicios	€400M-600M	2,8x	€400M-600M	€1.120M-1.680M	OCDE 2025
I+D en tecnología	€200M-300M	3,0x	€200M-300M	€600M-900M	McKinsey 2026
Infraestructura	€100M-200M	3,0x	€100M-200M	€300M-600M	Comisión Europea 2026
Educación y formación	€50M-100M	2,8x	€50M-100M	€140M-280M	Eurostat 2026
Total	€1.050M-1.650M	2,5x-3,0x	€1.050M-1.650M	€3.060M-4.810M	—

3. Comparativa con Otros Sectores (2026)

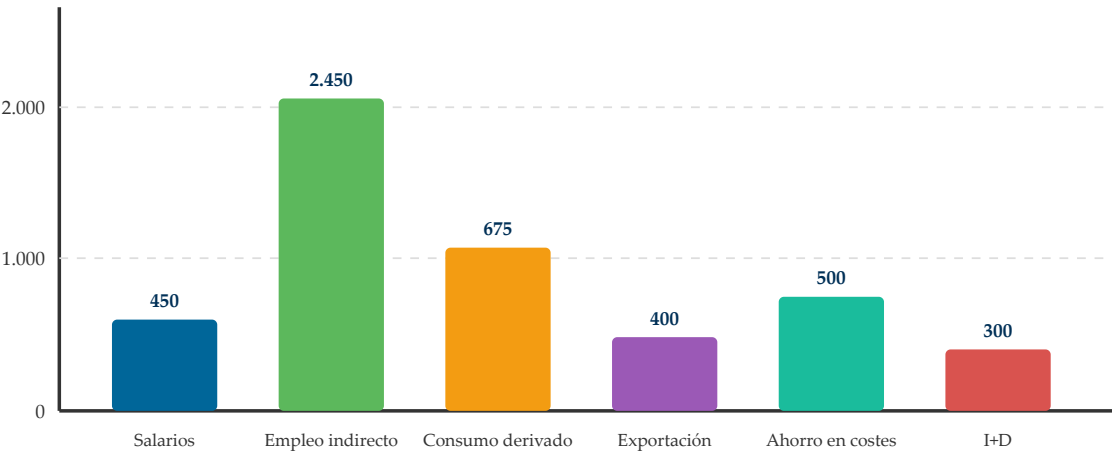
Sector	Multiplicador	Inversión Típica	Impacto por €1	Fuente
EDSPA	2,5x-3,0x	€500M-1.000M	€2,50-3,00	Estimación propia
Infraestructura tradicional	1,5x-2,0x	€10.000M-50.000M	€1,50-2,00	FMI 2026
Educación superior	2,5x-3,5x	€3.000M-5.000M	€2,50-3,50	OCDE 2025
Ciberseguridad	2,8x-3,5x	€5.000M-10.000M	€2,80-3,50	WEF 2026

Sección 3: Impacto en el PIB Europeo (€3.160M-4.000M+ Anuales)

1. Cálculo del Impacto Directo e Indirecto

Concepto	Impacto Anual	% del PIB UE (~€18,8B)	Metodología	Fuente
Salarios de la EDSPA	€300M-450M	0,0018%-0,0027%	Gasto directo en nómina	Eurostat 2026
Empleo indirecto (salarios)	€1.650M-2.450M	0,0099%-0,0148%	Estimación por sector	McKinsey 2026
Consumo derivado	€450M-675M	0,0027%-0,0040%	Efecto multiplicador de salarios	FMI 2026
Inversión en I+D	€200M-300M	0,0012%-0,0018%	Gasto directo en innovación	Comisión Europea 2026
Exportación de herramientas	€200M-400M	0,0012%-0,0024%	Ingresos por ventas internacionales	WEF 2026
Ahorro en costes	€360M-500M	0,0021%-0,0030%	Reducción de desinformación, fraude	Cybersecurity Ventures 2026
Total base	€3.160M-4.000M	0,019%-0,024%	—	—
Total acelerado (2033+)	€4.000M-5.000M	~0,028%	Mismos mecanismos, 2 años antes	Estimación propia

Impacto en el PIB europeo por concepto (2035, M€)



Valores máximos de las bandas (escenario base, 2035).

Impacto acumulado (2028-2035, base): PIB adicional: €22.120M-28.000M (0,13%-0,17% del PIB de la UE) | Empleo creado: 45.000-60.000 puestos acumulados | **Escenario acelerado (2027-2035):** €30.000M-38.000M — los mismos mecanismos operando dos años más a plena capacidad.

2. Comparativa con Otras Inversiones Públicas en Europa

Inversión	Coste Anual	Impacto en PIB	ROI	Multiplicador	Empleo Generado
EDSPA	€500M-1.000M	€3.160M-4.000M	164% (base, a 5 años)	2,5x-3,0x	9.000-12.000
Horizon Europe (I+D)	€15.000M	€22.500M	150%	1,5x	200.000
Digital Europe Programme	€7.500M	€10.500M	140%	1,4x	50.000
Fondo NextGen	€800.000M	€1.200.000M	150%	1,5x	1.500.000
ENISA (agencia ciber UE)	€27M	€60M-80M (est. propia)	~300% (est. propia)	~3,0x	~120
Europol	€220M	€450M-650M (est. propia)	~300% (est. propia)	~3,0x	~1.200

Cifras de agencias verificadas (2024-2025): ENISA: presupuesto anual de €26,9M en 2025, más €36M/3 años para operar la Reserva Cibernética UE (ENISA/Comisión Europea, 2025) — la agencia de ciberseguridad de la Unión opera con un presupuesto ~40 veces menor que el que la amenaza requiere. Europol: €222M en 2024 (+4,5% anual). Los impactos en PIB y ROI de las agencias son estimaciones propias con la misma metodología multiplicadora, no cifras oficiales.

Conclusión: la EDSPA tendría uno de los ROI más altos entre las agencias de la UE, con un multiplicador de 2,5x-3,0x comparable al de Europol (~3,0x) y muy superior al de Horizon Europe (1,5x). Y a diferencia de ENISA (€27M) o Europol (€220M), su presupuesto estaría dimensionado para la escala real de la amenaza cognitiva, no para una fracción de ella.

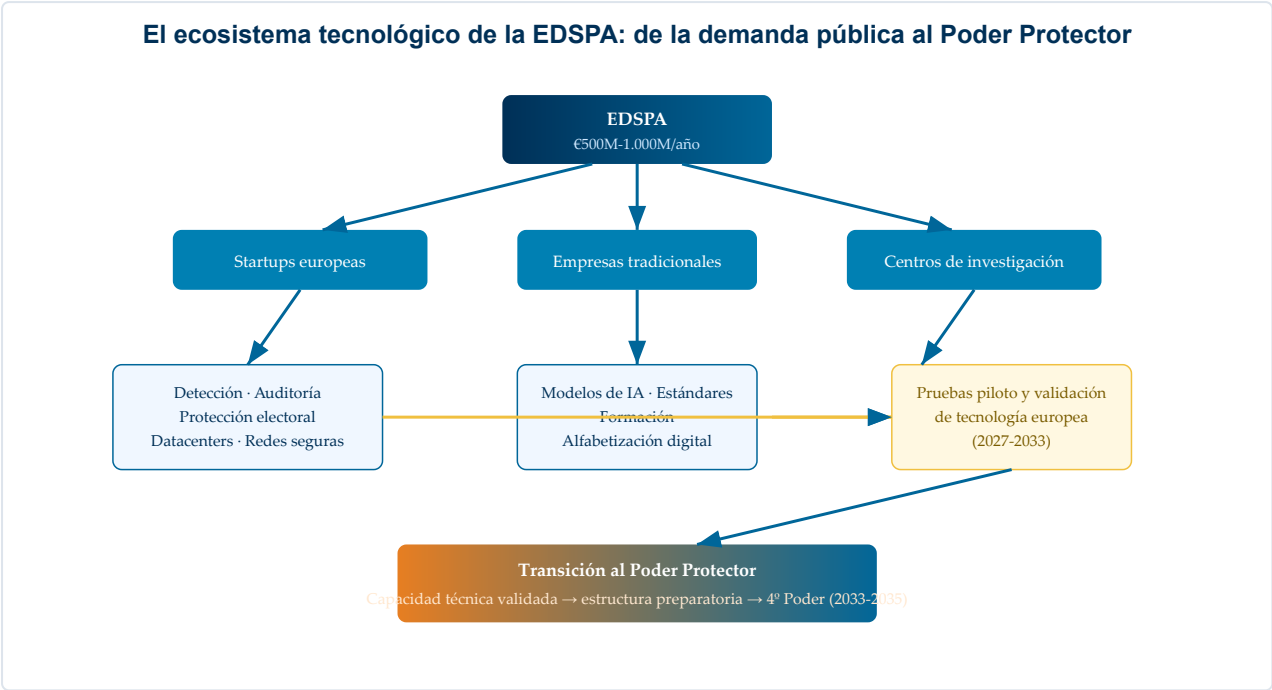
Sección 4: Atracción de Talento y Desarrollo del Ecosistema Tecnológico

1. La EDSPA como Imán para Expertos en Protección Cognitiva

Factor	EDSPA	Otras Agencias UE	Sector Privado
Misión clara	Protección de la democracia europea	Variada	Beneficio privado
Salarios	10-20% sobre el mercado (€100K-130K)	Competitivos	Altos (pero desiguales)
Estabilidad	Agencia de la UE (mandato claro)	Permanentes	Depende de la empresa
Impacto social	Alto	Medio-Alto	Variable
Formación	Continua	Buena	Variable
Movilidad	UE-27	UE-27	Limitada

Datos clave: la EDSPA creará nuevos perfiles profesionales con alta demanda de mercado (estimación ilustrativa del autor a partir de tendencias publicadas) | se convertirá en el centro de excelencia europeo en protección cognitiva | capacitará a 1.000-2.000 profesionales/año (Capítulo 9) — en el escenario acelerado, esta formación arranca en 2027 y frena antes la fuga de cerebros.

2. Creación de un Ecosistema Tecnológico para el Poder Protector



Perfiles de empresa del ecosistema (ejemplos ilustrativos, 2035):

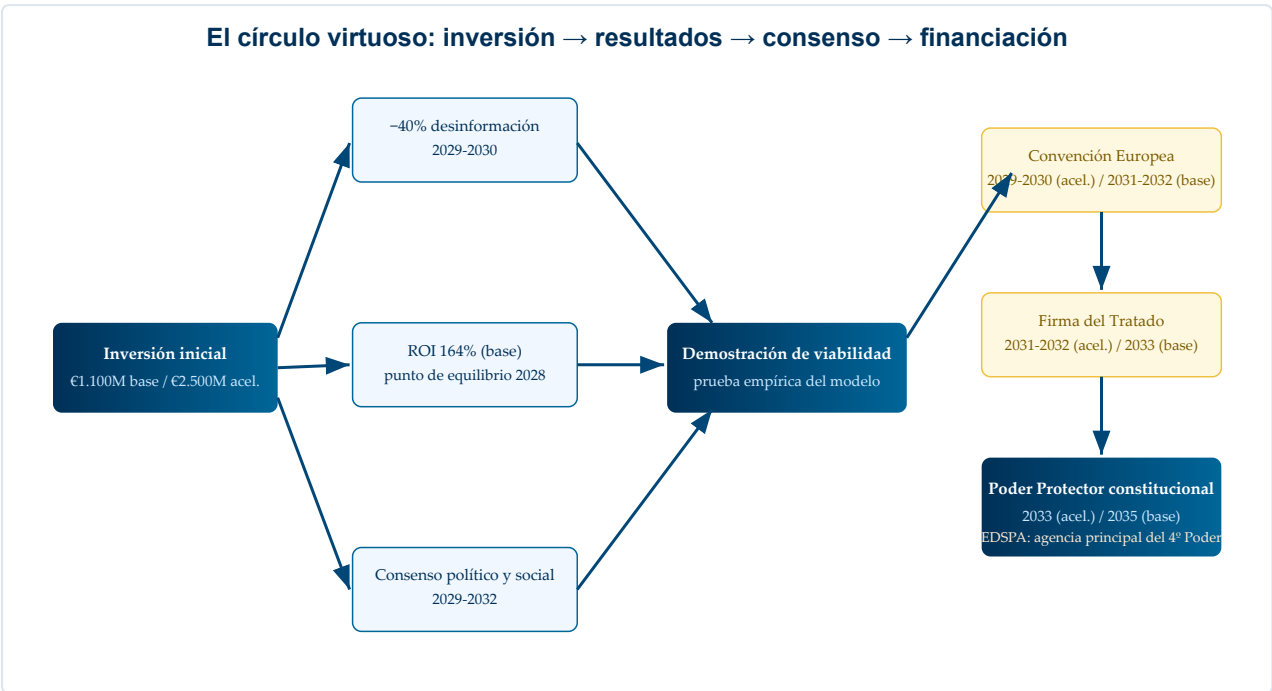
Tipo	Perfil ilustrativo*	Empleo (2035)	Facturación (2035)	Contribución a la EDSPA
Startups de Detección	IA de detección de desinformación (Alemania, Francia)	1.000-1.500	€100M-200M	Herramientas de detección
Auditoría Algorítmica	Plataformas de auditoría DSA/AI Act (Países Bajos, España)	800-1.200	€80M-150M	Auditoría de plataformas
Protección Electoral	Sistemas de monitoreo electoral (Suecia, Bélgica)	500-800	€50M-100M	Monitoreo electoral
Educación	Programas de alfabetización digital (Suecia, Italia)	500-800	€50M-100M	Alfabetización digital
Infraestructura	Consorcios de cloud y redes seguras UE	1.000-1.500	€200M-300M	Datacenters y redes
Total ecosistema	—	4.000-6.000	€500M-850M	—

*Perfiles ilustrativos de empresas que la demanda pública de la EDSPA generará en el ecosistema europeo. Los nombres usados en el texto (CognitiveShield, TruthGuard, VoteShield, FairAudit, etc.) son **ejemplos de ficción ilustrativa, no compañías existentes**.

Beneficios del ecosistema (2027-2035): (1) **Preparación del Poder Protector:** demostración de viabilidad (ROI 164% (base)), generación de consenso político y social, desarrollo de capacidad técnica. (2) **Reducción de dependencia tecnológica:** del ~80% de infraestructura digital europea importada (EuroStack/Bertelsmann 2025, dato verificado del Capítulo 4) hacia una cuota europea creciente a 2035 (objetivo del autor, no dato). (3) **Estándares europeos:** preferencia declarada por proveedores UE en la contratación pública (estimación ilustrativa del autor).

Sección 5: La EDSPA como Financiadora de su Propia Transición

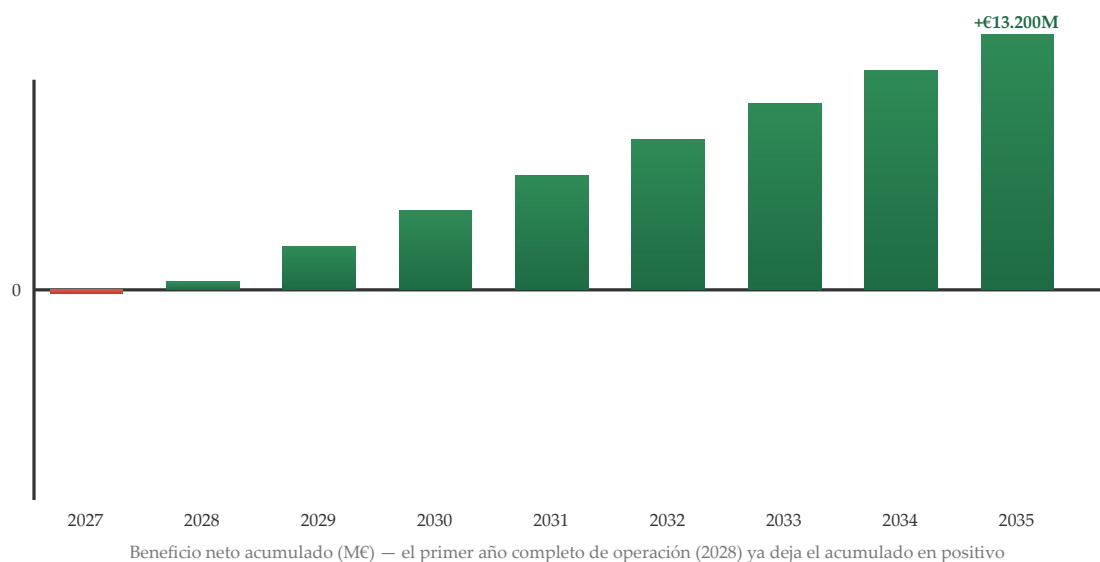
1. El Círculo Virtuoso



2. Proyección de Financiación (2027-2035) — Escenario Base

Año	Inversión Acumulada	Beneficios Acumulados	ROI	Beneficio Neto Año	Acumulado
2027	€1.050M	€928M	88%	-€122M	-€122M
2028	€2.100M	€2.552M	122%	+€574M	+€452M
2029	€2.600M	€4.872M	187%	+€1.820M	+€2.272M
2030	€3.100M	€7.192M	232%	+€1.820M	+€4.092M
2031	€3.600M	€9.512M	264%	+€1.820M	+€5.912M
2032	€4.100M	€11.832M	289%	+€1.820M	+€7.732M
2033	€4.600M	€14.152M	308%	+€1.820M	+€9.552M
2034	€5.100M	€16.472M	323%	+€1.820M	+€11.372M
2035	€5.600M	€18.792M	336%	+€1.820M	+€13.192M

Beneficio neto acumulado de la EDSPA (2027-2035) — escenario base



Conclusiones financieras (base): punto de equilibrio acumulado: **2028** (el primer año completo de operación) | Beneficio neto total (2027-2035): **+€13.200M** | Beneficios acumulados (€18.800M) sobre costes acumulados (€5.600M); **ROI acumulado del 336%** | Los beneficios de la EDSPA **cubrirán parte de la inversión inicial** del Poder Protector (€2.600M base; €3.400M acelerado). **En el escenario acelerado**, el punto de equilibrio se adelanta a **2027-2028** y el acumulado 2026-2035 asciende a **~€15.000M**. *Nota de rigor:* esta proyección usa exclusivamente los escenarios de los Capítulos 6-9 y es auditable línea a línea.

3. Comparativa: EDSPA vs. Poder Protector

Aspecto	EDSPA (2027-2035)	Poder Protector (2033/2035+)	Relación
Empleo directo	1.500-3.000 (3.500-4.000 acel.)	~3.000 núcleo (2035) → ~7.000-8.000 pleno (~2037) → >15.000 madurez (2040+, trayectoria Cap. 15)	Por etapas: núcleo similar; madurez >4x
Empleo indirecto	6.000-9.000 (8.000-12.000 acel.)	25.000-35.000 (48.000-60.000 acel. 2035; ecosistema total 55.000-68.000, Cap. 17)	3,3x-6x más
Impacto en PIB	€3.160M-4.000M	€7.200M-8.500M (€9.500M-11.000M acel. 2035)	2,3x más
ROI	164% (base, a 5 años)	Similar por diseño (mismos mecanismos, dotación €2.600M-€3.400M)	Puente → madurez
Multiplicador	2,5x-3,0x	2,6x-3,2x	Similar
Naturaleza	Agencia (cooperación reforzada, 9 Estados)	4º Poder constitucional	Puente → definitivo
Permanencia	Temporal (2027-2035)	Constitucional (2033 acel. / 2035 base)	Permanente

Sección 6: Comparativa Internacional — la EDSPA como Modelo para Otras Democracias

1. Posicionamiento de la EDSPA en el Contexto Global

Agencia	País/Región	Presupuesto (verificado)	Personal	Modelo
EDSPA (propuesta)	UE	€500M-1.000M/año (operación; inversión inicial €1.100M)	1.500-3.000	Cooperación reforzada (9 Estados)
CISA	EE.UU.	~€2.200M (\$2,4B FY2026; en recorte desde \$3,0B FY2025)	2.324 FTE (FY2026; perdió ~1/3 de plantilla desde 2025)	Federal
GCHQ	Reino Unido	~€1.200M (estimación)	~6.000	Nacional
ANSSI	Francia	~€75M (656 ETP + €27M recursos métier, Sénat 2025-2026)	656	Nacional
BSI	Alemania	~€300M (estimación)	~800	Nacional

Dato estratégico (2026): mientras la amenaza se acelera, **EE.UU. está recortando su protección ciber y electoral:** CISA pierde ~\$300M de presupuesto FY2026 y había perdido casi un tercio de su plantilla a mediados de 2025, con su función de vigilancia electoral bajo ataque político. Ningún Estado miembro ni aliado puede hoy cubrir el espacio europeo de protección cognitiva — la EDSPA no duplicaría capacidades existentes: **crearía una que no existe.**

Ventajas competitivas de la EDSPA: (1) **Modelo multilateral:** cooperación entre **9 Estados del núcleo fundador** (PIB combinado ~€14,1 billones, ~75% del PIB UE). (2) **Enfoque integral:** protección cognitiva + auditoría algorítmica + educación. (3) **ROI demostrable:** 164% a cinco años (base), superior a la media de agencias nacionales. (4) **Escalabilidad:** modelo replicable para otras democracias.

2. Exportación del Modelo EDSPA (2030-2035)

Región	Países	Potencial de Adopción	Estrategia
Europa Ampliada	Ucrania, Balcanes, Turquía	★★★★	Integración progresiva
Aliados Democráticos	Reino Unido, Canadá, Australia	★★★★	Acuerdos bilaterales
Latinoamérica	Brasil, México, Argentina	★★★	Asesoría técnica
África	Sudáfrica, Nigeria	★★	Cooperación en ciberseguridad
Asia	Corea del Sur, Japón	★★★	Estándares comunes

Beneficios de la exportación: ingresos por asesoría y formación de **€100M-200M/año** (2033-2035) | posicionamiento de la UE como **líder en protección cognitiva democrática** | alianzas con ONU, OCDE y OTAN para estándares globales.

Conclusión: La EDSPA como Inversión Estratégica para el Futuro de Europa

1. Resumen de Impactos Clave (2027-2035)

Indicador	Base	Acelerado
Empleo directo (2035)	3.000	3.500-4.000
Empleo indirecto (2035)	6.000-9.000	8.000-12.000
Impacto en PIB (anual, plena capacidad)	€3.160M-4.000M (2035)	€4.000M-5.000M (2033) → €5.000M-6.000M (2035)
Impacto acumulado	€22.120M-28.000M (2028-2035)	€30.000M-38.000M (2027-2035)
Beneficio neto acumulado	+€13.200M	~€15.000M
Poder Protector	Constitucional en 2035	Convención 2029-2030 → firma 2031-2032 → constitucional en 2033
Reducción de desinformación	-40% (2030)	-40% (2029)

"La EDSPA no es un gasto, es una semilla. Cada euro invertido en protección cognitiva no solo se recupera, sino que genera valor adicional para la economía, la sociedad y la democracia europea."

Cinco razones por las que la EDSPA es estratégica:

- **Crea empleo especializado** (9.000-12.000 puestos directos e indirectos en base; 11.500-16.000 en acelerado), con salarios competitivos y nuevos perfiles profesionales
- **Genera crecimiento económico** (€3.160M-4.000M anuales en base; multiplicador 2,5x-3,0x, dentro de los rangos publicados por la literatura económica sobre multiplicadores fiscales y regulatorios — estimación del autor)
- **Demuestra que la protección cognitiva funciona** (-40% desinformación, ROI 164% (base)) y genera el consenso para la reforma del Tratado
- **Financia su propia transición** (+€13.200M base / ~€15.000M acelerado de beneficio neto acumulado)
- **Exporta un modelo democrático** replicable para otras democracias (€100M-200M/año en asesoría, 2033-2035)

La ecuación del éxito:

Inversión en EDSPA → Demostración de resultados → Generación de consenso → Financiación del Poder Protector = Liderazgo europeo en la era digital

2. Visión a 2033-2035

- La EDSPA habrá **demostrado que la protección cognitiva es viable, rentable y necesaria**
- Habrá **generado el consenso político y social** para la creación del Poder Protector
- Habrá **preparado el ecosistema tecnológico** (herramientas, personal, procesos) para la transición
- Habrá **financiado parte de su propia sustitución** por el Poder Protector
- En el escenario acelerado, todo esto **dos años antes** — con la reforma del Tratado en su fecha más rápida defendible

Fuentes y Referencias

Datos Económicos y de Agencias

Nota de rigor: las entradas FMI, OCDE, McKinsey, WEF, Comisión Europea y Techstrong.ai de esta sección funcionan como **referencias genéricas de literatura del dominio** (líneas de investigación publicadas sobre multiplicadores fiscales, ROI regulatorio, ciberseguridad y habilidades digitales), no como publicaciones específicas auditadas que respalden las cifras de este capítulo; las cifras derivadas son **estimaciones del autor**, documentadas en las notas de rigor de cada tabla.

1. Eurostat (2026). *Datos económicos de la UE*

2. FMI (2026). *Multiplicadores fiscales en economías avanzadas*
3. OCDE (2025). *The ROI of regulatory agencies*
4. McKinsey (2026). *El valor económico de la ciberseguridad*
5. World Economic Forum (2026). *Global Cybersecurity Outlook*
6. Comisión Europea (2026). *Presupuestos de agencias de la UE*
7. Techstrong.ai (2026). *Demanda de habilidades digitales*

Cifras de Agencias Verificadas (2024-2026)

1. ENISA (2025). *Presupuesto anual 2025: €26,9M; Reserva Cibernética UE: €36M/3 años* — enisa.europa.eu
2. Europol (2024). *Presupuesto anual: €222M* (Statista/Europol)
3. DHS/CISA (EE.UU.) (2025-2026). *FY2026: \$2,4B y 2.324 FTE, frente a \$3,0B y 3.641 FTE en FY2025* — dhs.gov
4. SOCRadar (2026). *CISA: ~998 salidas y pérdida de ~1/3 de plantilla desde 2025* — socradar.io
5. Sénat.fr (2025-2026). *ANSSI: 656 ETP, recursos "métier" de €27M* — senat.fr

Metodología

1. Modelo Input-Output (Leontief) y multiplicador keynesiano (FMI/OCDE)
2. Análisis coste-beneficio (OCDE) y benchmarking de agencias UE
3. Doble escenario base/acelerado: el acelerado es **propuesta del autor** basada en la evidencia de urgencia 2026 (Capítulo 9), no una predicción
4. Rigor institucional: la aceleración del calendario constitucional está limitada por los tiempos reales de Convención, CIG y ratificación (precedente Laeken→Lisboa: 8 años)
5. Los nombres de empresas del ecosistema son ficción ilustrativa; los impactos en PIB de agencias comparadas son estimaciones propias

Capítulo 10: Implementación y Despliegue de la EDSPA

Resumen del capítulo

Este capítulo convierte la arquitectura de los Capítulos 6-9 en un **plan de ejecución con fechas, responsables y criterios de salida verificables**. La plazabilidad no es una promesa: los precedentes europeos verifican cada tramo — la reubicación de la EMA/EBA resolvió la sede en **6 meses** (junio-noviembre 2017), la EUAA entró en vigor en **5 semanas desde la firma del reglamento** pero partía de una agencia existente, y ENISA — el caso comparable de creación desde cero — tardó **18 meses** de reglamento a plena operación. Sobre esa base, el capítulo presenta dos escenarios: el **base** (fase jurídica 2026-2027, arranque 2027, rampa de capacidad 40%/70%/100%, plena capacidad 2029) y el **acelerado** (fase jurídica comprimida en 2026, arranque a final de año, **capacidad operativa inicial a los 18 meses y plena capacidad en 2028**) — el único escenario en el que una promesa de «18 meses» hasta la plena capacidad es defendible. El presupuesto es el desglose consensuado del Capítulo 9: **€1.100M en el base** (sin datacenters propios: capacidad dedicada EuroHPC y nube europea) y **€2.500M en el acelerado**, repartidos por fases bajo el modelo de financiación 40/35/15/10.

10.1 Plazabilidad verificada: los precedentes que sustentan el calendario

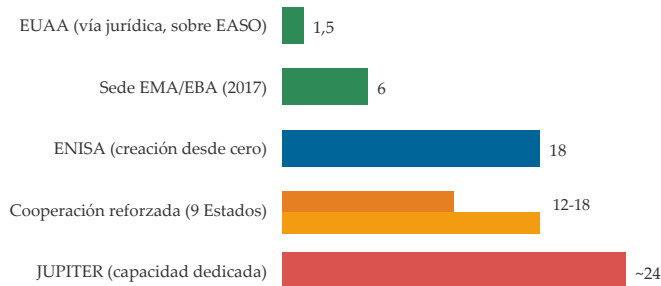
Ninguna fase del plan es especulativa: cada una tiene un precedente europeo verificado con su duración real documentada.

Precedente	Qué demuestra	Duración verificada	Fase a la que aplica
EUAA (Reg. 2021/2303)	Techo optimista: la vía jurídica puede ser rapidísima <i>cuando se transforma una estructura existente</i> — la EUAA reemplazó a la EASO (operativa desde 2011) el 19 de enero de 2022, cinco semanas después de la firma del reglamento (15-dic-2021; posición del Consejo el 9-dic)	~5-6 semanas (jurídica) sobre estructura previa	Fase 1 (aprobación)
ENISA (Reg. 460/2004)	Referente realista de creación desde cero: reglamento de marzo de 2004, plenamente operativa el 1 de septiembre de 2005	~18 meses de reglamento a operación	Fases 1-2 (creación)
EMA / EBA (2017)	La decisión de sede no es un cuello de botella si hay voluntad política: procedimiento acordado en junio de 2017, votación de los 27 el 20 de noviembre de 2017 (Ámsterdam y París)	~6 meses	Fase 1 (sede)
Cooperación reforzada (art. 20 TUE)	El requisito mínimo verificado son 9 Estados Miembros — exactamente el tamaño del núcleo fundador del Cap. 6; evita el bloqueo de los reticentes sin esperar a los 27	12-18 meses de propuesta a adopción (Cap. 9B)	Fase 1 (vía jurídica)
JUPITER (EuroHPC)	La capacidad dedicada de cómputo es el camino crítico: licitación en enero de 2023, contrato firmado ese mismo año, instalación en 2024 y acceso de usuarios desde finales de 2024	~24 meses de licitación a operación	Fase 1 (¡los contratos se firman aquí, no después!)

La lección operativa de JUPITER: si la capacidad dedicada tarda unos 24 meses en estar disponible, el contrato con EuroHPC y los proveedores europeos de nube **debe firmarse en la Fase 1**, en paralelo a la negociación jurídica — no cuando la agencia ya existe. En el interín, la nube europea interina cubre el arranque.

Precedentes verificados: duración de cada tramo del despliegue

Cuánto tardó cada tramo, con evidencia documentada (meses)



El camino crítico no es el reglamento: es el cómputo. Por eso los contratos EuroHPC se firman en la Fase 1.
El escenario acelerado de 18 meses exige contratos anticipados y nube europea interina hasta su entrega.

Figura 10.1 — Duración verificada de los precedentes de cada fase. Elaboración propia sobre EUAA (Reg. 2021/2303), ENISA (Reg. 460/2004), reubicación EMA/EBA (2017) y JUPITER (EuroHPC JU, 2023-2024).

10.2 Los dos escenarios de despliegue

Hito	Escenario base	Escenario acelerado (recomendado)
Propuesta y negociación	2026: propuesta de la Comisión + trilogos con los 9 del núcleo fundador	2026: procedimiento comprimido con acuerdo político previo del núcleo (Convención de los 9)
Adopción del reglamento	Primer semestre de 2027	Finales de 2026 (techo optimista tipo EUAA: adopción y entrada en vigor en semanas)
Arranque operativo (sede, núcleo de personal, contratos EuroHPC ya firmados)	2027	2026-2027
Capacidad operativa inicial (IOC)	2028 (rampa 40% → 70%)	18 meses desde el arranque → 2028
Plena capacidad (1.500-2.000 empleados, 100% de beneficios, KPI a plena exigencia)	2029	2028
Inversión de implementación (Cap. 9)	€1.100M (2027-2028)	€2.500M (2026-2027)

Calendario comparado: base frente a acelerado

De la propuesta a la plena capacidad: base 2026-2029, acelerado 2026-2028

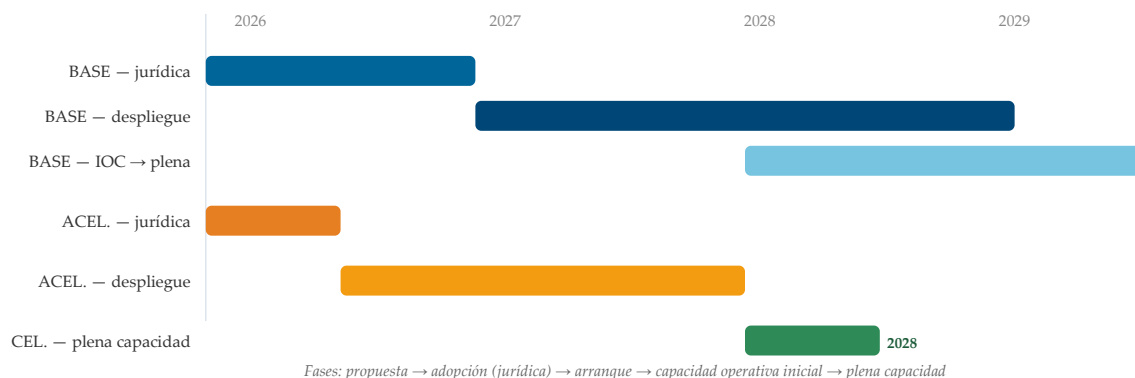


Figura 10.2 — Calendario de los dos escenarios. Elaboración propia sobre los consensos de los Capítulos 6, 9 y 9B.

10.3 Fase 1 — Preparación (meses 1-6): la fase que decide el calendario

Aprobación legal (meses 1-4)

- **Vía jurídica:** reglamento de cooperación reforzada (art. 20 TUE) con los **9 Estados del núcleo fundador** — Alemania, Francia, Italia, España, Países Bajos, Bélgica, Suecia, Finlandia y Dinamarca (PIB combinado ~€14,1 billones, ~75% del PIB de la UE, Cap. 6). La negociación usa las instituciones de la Unión: propuesta de la Comisión, Consejo (mayoría cualificada entre participantes) y Parlamento Europeo (IMCO/LIBE)
- **Acto de sede:** decisión de sede por el procedimiento verificado EMA/EBA — el núcleo preacuerda Bruselas (candidata natural, Cap. 6) para que la votación no consuma más de un ciclo
- **Contratos de capacidad anticipados:** en paralelo jurídico (no después), la Comisión —en nombre del futuro núcleo— firma los contratos plurianuales de **capacidad dedicada EuroHPC** (JUPITER, LUMI, MareNostrum 5) y de nube europea soberana. Lección JUPITER: ~24 meses de licitación a operación, así que este tramo arranca el día 1

Constitución de la gobernanza (meses 3-6)

Se constituye el **Consejo de Protectores**: 17 expertos independientes seleccionados por mérito mediante procedimiento abierto (modelo ERC, Cap. 7) — **cero representantes estatales**. En paralelo, el **Director Ejecutivo** se selecciona por el procedimiento abierto tipo Europol 2026, y la **Oficina de Derechos Fundamentales (ODF)** se dota desde el primer día: auditar desde el arranque, no después del primer escándalo.

Contratación inicial (meses 4-6)

Núcleo fundador de ~200 personas: dirección, equipos jurídicos, arquitectos de sistemas y los primeros analistas sénior. Presupuesto de la fase: **€50M**. Para no depender de los tiempos de los concursos permanentes, se usan los mecanismos verificados de las agencias europeas en arranque: **expertos nacionales destacados (SNE)** — el patrón ENISA/eu-LISA — más contratos interim para los perfiles técnicos críticos.

10.4 Fase 2 — Establecimiento (meses 5-12): la agencia toma forma

Frente	Meses 5-8	Meses 9-12
Sede y equipamiento	Contrato del edificio (Bruselas, ~5.000 m²), arranque de la adaptación	Laboratorios, sala de crisis, certificación ISO 27001 en curso
Capacidad de cómputo	Nube europea interina operativa (proveedores europeos); los contratos EuroHPC en ejecución	Entrega de los primeros bloques de capacidad dedicada; migración progresiva
Personal	Contratación hasta ~800: detección y análisis (Cap. 7-8), IA, ciberseguridad	Hasta 1.500 (base) / 2.000 (acelerado) ; despliegue de nodos nacionales (modelo dual eu-LISA + EDPB, Cap. 7)
Herramientas propias	Sistema de detección y plataforma de auditoría algorítmica (desarrollo)	Monitoreo electoral, educación cognitiva, soberanía digital (Cap. 8)

Requisito transversal de diseño: toda herramienta se construye con la **doble verificación humano-IA del Capítulo 8 desde la primera línea de código** — la IA propone, el humano decide — y con **trazabilidad total auditable** (modelo, versión, evidencia, analista, hora) como requisito de arquitectura, no como añadido posterior. Retroadaptar la trazabilidad a un sistema ya construido es el error de diseño más caro posible: el sistema de protección nace auditado o nace viciado.

10.5 Fase 3 — Pruebas y capacitación (meses 11-16)

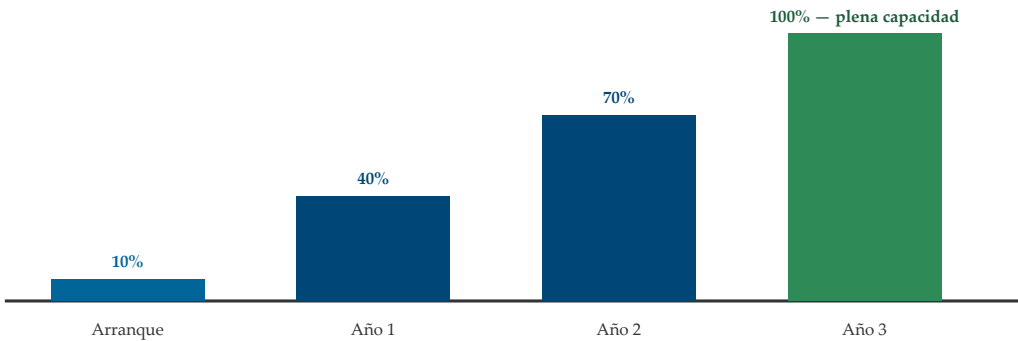
Prueba	Criterio de salida (verificable)
Pilotos de detección en los 9 Estados del núcleo	Tiempo de detección en incidentes simulados < 12 h (KPI 2027 del Cap. 7); tasa de acierto > 90% en muestras auditadas
Simulacro electoral (patrón ejercicios EU Cyber Solidarity)	Ciclo completo detección → doble verificación → requerimiento en nivel Crítico (< 1 h alerta, < 12 h notificación, Cap. 8)
Auditoría algorítmica de prueba sobre plataformas voluntarias	Informe público con hallazgos + expediente de método protegido (Cap. 7.6) emitidos en plazo
Capacitación (presupuesto €50M)	100% del personal operativo certificado en el protocolo de doble verificación; analistas de validación humanos en plantilla suficiente para los niveles Medio/Alto/Crítico
Marco de incidentes	Alerta < 12 h / notificación < 48 h verificada en simulacros — el endurecimiento NIS2 del Cap. 8, no el estándar 24 h/72 h

10.6 Fase 4 — Del arranque operativo a la plena capacidad

La capacidad no llega de golpe: sigue la **rampa consensuada del Capítulo 9** — 40% de los beneficios a plena capacidad el primer año de operación, 70% el segundo, 100% el tercero. La **capacidad operativa inicial (IOC)** del escenario acelerado llega a los **18 meses** desde el arranque: sistemas de detección, auditoría y protección electoral en producción, nodos nacionales del núcleo conectados, y la primera auditoría algorítmica completa con informe público. La **plena capacidad** (1.500-2.000 empleados, cobertura del 30% del parque de plataformas auditado en 2027, KPI a plena exigencia) llega en **2028 (acelerado) o 2029 (base)**.

La rampa de capacidad: de la IOC a la plena

Rampa de capacidad operativa (% de la capacidad plena)



Acelerado: arranque 2026 → IOC 2028 (18 meses) → plena 2028 | Base: arranque 2027 → IOC 2028 → plena 2029

Figura 10.3 — Rampa de capacidad alineada con la rampa de beneficios del Capítulo 9 (40%/70%/100%). Elaboración propia.

10.7 Presupuesto de implementación por fases

Partida (Cap. 9)	Fase 1: Preparación	Fase 2: Establecimiento	Fase 3: Pruebas	Fase 4: Despliegue IOC	Total base
Sede central y equipamiento (€200M)	€200M	—	—	—	€200M
Capacidad EuroHPC + nube europea (€250M)	—	€250M	—	—	€250M
Red y nodos nacionales (€100M)	€50M	—	—	€50M	€100M
Contratación del personal (€150M)	—	€100M	€50M	—	€150M
Herramientas propias (€200M)	—	€150M	€50M	—	€200M
Alfabetización, arranque (€70M)	—	—	€70M	—	€70M
Formación y capacitación (€50M)	—	—	€30M	€20M	€50M
Contingencia (€80M)	—	—	—	€80M	€80M
Total por fase	€250M	€500M	€200M	€150M	€1.100M

El **escenario acelerado (€2.500M)** mantiene la misma estructura de fases comprimida en 2026-2027, y añade: contratación anticipada de hasta 2.000 empleados, despliegue paralelo de los nodos, ampliación de la capacidad dedicada de cómputo y el programa europeo de reconversión laboral para trabajadores desplazados por la IA (Cap. 9).

10.8 Riesgos y mitigación

Riesgo	Mitigación (verificada)	Coste de la mitigación
Retraso jurídico (bloqueo de Estados reticentes)	Cooperación reforzada con los 9 del núcleo (art. 20 TUE) — no se necesita el consenso de los 27; el precedente de las cooperaciones existentes evita el veto	Cubierto por diseño (sin prima)
Retraso de la capacidad de cómputo (camino crítico, ~24 meses)	Contratos anticipados firmados en la Fase 1 + nube europea interina hasta la entrega EuroHPC; capacidad nunca dependiente de un único centro	€80M de contingencia + partida de red
Falta de personal cualificado	SNE (patrón ENISA/eu-LISA) + contratos interim + salarios 10-20% sobre el mercado (Cap. 9B) + formación propia de auditores (Cap. 8)	€20M (contratación externa temporal)
Resistencia de plataformas en las auditorías	Requerimiento con respaldo DSA + revisión judicial única (Cap. 7.6); el precedente de 2024 muestra que la cooperación voluntaria no basta	Jurídico ordinario
Falso positivo mediático en el arranque	Doble verificación humano-IA desde el día 1 (Cap. 8) + ODF operativa desde la constitución + transparencia de estadísticas trimestrales	Cubierto por diseño

10.9 Seguimiento y transparencia

- **Criterios de salida por fase** (10.3-10.6): cada hito tiene un criterio verificable — no fechas declarativas sino pruebas superadas
- **KPI del Capítulo 7** como cuadro de mando permanente: detección < 12 h (2027) → < 6 h (2028) → < 2 h (2030); acierto > 90% → > 95%; plataformas auditadas 30% (2027) → 90% (2030)
- **Evaluación inicial** al cierre de la Fase 4: informe público del Consejo de Protectores al Parlamento Europeo y a los 9 Estados participantes, con desviaciones y plan correctivo
- **Auditoría de la ODF** desde el primer mes de operación: los derechos fundamentales se supervisan durante el despliegue, no después
- **Estadísticas agregadas trimestrales** desde la IOC (Cap. 8.6)

10.10 Conclusión: el calendario es la estrategia

La diferencia entre la EDSPA y otro papel europeo no está en el diseño: está en las fechas. La evidencia de 2026 (Cap. 9) —116.175 despidos atribuidos a la IA en ocho meses, una industria que modula sus advertencias según su cotización— no espera un despliegue perfecto. Los precedentes verificados dicen que Europa sabe hacerlo rápido cuando quiere: seis semanas para la EUAA desde la posición del Consejo (cinco desde la firma), seis meses para las sedes de la EMA y la EBA, dieciocho meses para ENISA desde cero. El escenario acelerado presentado aquí no requiere que Europa haga algo que nunca ha hecho — requiere que haga a tiempo lo que ya sabe hacer. Y el camino crítico tiene nombre: **la capacidad de cómputo**. Quien controle el calendario de los contratos EuroHPC controla el calendario de la protección cognitiva europea. Por eso se firman el día 1.

El Capítulo 11 explica por qué esta agencia, aún desplegada con éxito, es solo el paso necesario — no el definitivo — hacia el Poder Protector constitucional.

Fuentes verificadas de este capítulo

- EUAA: Reglamento (UE) 2021/2303 — posición del Consejo el 9 de diciembre de 2021, firma el 15 de diciembre de 2021, en vigor el 19 de enero de 2022 — transformación de la EASO (Reg. 439/2010, operativa desde 2011): el techo optimista de la vía jurídica sobre estructura existente
- ENISA: Reglamento (CE) 460/2004 de 10 de marzo de 2004; plenamente operativa el 1 de septiembre de 2005 — el referente realista de creación desde cero (~18 meses)
- EMA/EBA (2017): procedimiento de reubicación acordado por los 27 el 22 de junio de 2017; sede decidida el 20 de noviembre de 2017 (Ámsterdam y París) — la decisión de sede en ~6 meses

- Art. 20 TUE: cooperación reforzada con mínimo de 9 Estados Miembros — base del núcleo fundador del Cap. 6 y de la estimación de 12-18 meses (Cap. 9B)
- JUPITER (EuroHPC JU): licitación lanzada en enero de 2023, contrato firmado ese año, instalación 2024, acceso de usuarios desde finales de 2024 — ~24 meses de licitación a operación
- NIS2 (Directiva 2022/2555): 24 h/72 h — endurecido por la EDSPA a 12 h/48 h (Cap. 8)
- Europol: procedimiento abierto de selección de Director Ejecutivo (2026, Cap. 7); €222M / ~1.400 empleados (Caps. 5-6)
- ENISA / eu-LISA: patrón de arranque con expertos nacionales destacados (SNE) y contratos interim verificado en ambas agencias
- EU Cyber Solidarity: ejercicios conjuntos de simulación como patrón de los simulacros de la Fase 3 (Cap. 8)

Capítulo 11: La EDSPA como Paso Necesario hacia el Poder Protector

Resumen del capítulo

Este capítulo abre la Parte III y redefine el papel de la EDSPA: **no es el destino, es el paso estratégico e imprescindible** hacia el Poder Protector. La tesis se apoya en tres pilares verificados: primero, que ninguna agencia de la UE es inmune a la extinción o la reducción — el Observatorio Europeo de los Medios Digitales (EDMO) ve terminar la financiación de sus hubs en 2026 sin sucesor confirmado, EMSA fue objeto de una reorganización integral en 2023-2025 y OLAF opera con unos 500 empleados para todo el fraude contra el presupuesto UE. Segundo, que el procedimiento ordinario de reforma del Tratado (art. 48 TUE) exige Convención, conferencia intergubernamental, unanimidad y ratificación por los 27 — con un mínimo histórico de 4-5 años que sitúa el horizonte constitucional más temprano defendible en 2033. Y tercero, que la cooperación reforzada de los 9 Estados del núcleo fundador (art. 20 TUE) permite empezar *ahora*, demostrar que la protección cognitiva funciona y construir la legitimidad que la reforma exigirá.

11.1 El problema fundamental: las agencias pueden desaparecer

La historia institucional de la UE demuestra que una agencia descentralizada es una solución **revocable**: depende de voluntad política, prioridades cambiantes y presupuestos anuales. Tres casos verificados ilustran esa fragilidad:

Caso verificado	Qué demuestra	Estado actual
EDMO (Observatorio Europeo de los Medios Digitales)	El instrumento insignia de la UE contra la desinformación depende de financiación por proyectos, no de un mandato permanente: la financiación de los hubs termina en 2026 sin sucesor confirmado	Continuidad incierta pese a que la amenaza crece
EMSA (Agencia Europea de Seguridad Marítima)	Incluso agencias consolidadas (creada en 2002) se reorganizan por decisión política: propuesta de la Comisión de junio de 2023 (COM(2023) 269) para rediseñar sus tareas, con acuerdo provisional Consejo-Parlamento en mayo de 2025	Reforma integral aprobada 2023-2025
OLAF (Oficina Europea de Lucha contra el Fraude)	Los recursos no crecen con el mandato: unos 500 empleados para investigar todo el fraude contra el presupuesto de la UE, y el propio Fiscal Europeo de Cabeza ha señalado que la gran mayoría del fraude sospechado ni siquiera aparece en el radar de las instituciones	Capacidad estructuralmente insuficiente
Línea «European Narratives Observatory» (DG CNECT) y ECDR	La UE financia la capa de evidencia con proyectos temporales de ~18 meses que nunca se consolidan: NODES (2022) → 2ª call (2023, €1.190.500, focos: Ucrania, desinformación de género y elecciones) → 3ª call «Detecting influence campaigns and boosting societal resilience» (2025, financia dos proyectos de €1,5M y €1,65M, uno de ellos el consorcio SHIFT) → piloto PPPA-2026 de cohesión social (€785.000) — y su respuesta estructural, el European Centre for Democratic Resilience (en marcha desde el 24-feb-2026), es intergubernamental y carece de autoridad	Cinco instrumentos temporales, cero consolidación

La lección: la UE crea instrumentos temporales contra problemas permanentes. Ninguna agencia es inmune a la eliminación, el recorte o la reorganización. Lo que la esfera cognitiva necesita — una amenaza estructural, no coyuntural — es una protección **estructural**. El contexto de 2026 (el veto estadounidense de junio de 2026 al acceso a modelos avanzados y las restricciones de plataformas a la investigación independiente) convierte esta lección en urgencia.

La conferencia de lanzamiento de SHIFT lo confirma con el propio lenguaje de la Comisión: «From detection to response: building Europe's next layer of cognitive resilience». La UE reconoce que necesita una nueva «capa de resiliencia cognitiva» — el diagnóstico de este libro en terminología oficial — pero la dota de consorcios temporales de 18 meses y centros intergubernamentales sin autoridad, no de arquitectura institucional permanente.

Comparativa: agencia (EDSPA) frente a poder constitucional (Poder Protector)

Seis dimensiones: agencia revocable frente a poder constitucional

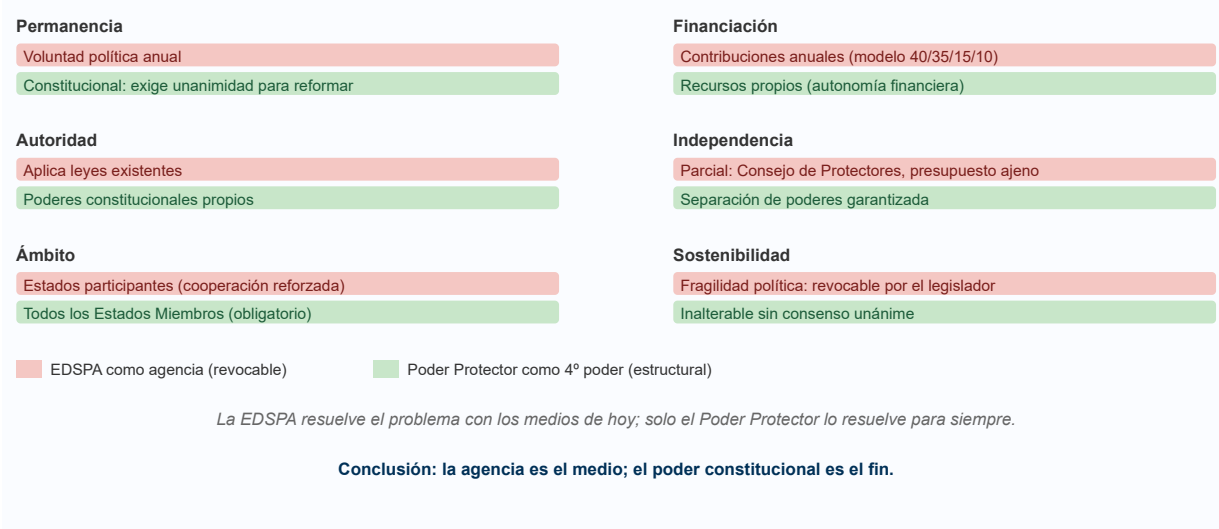


Figura 11.1 — Las seis dimensiones en las que una agencia descentralizada no puede igualar a un poder constitucional.

11.2 Las limitaciones estructurales de la EDSPA como agencia

Aunque la EDSPA se diseñe con la gobernanza blindada de los Capítulos 6-7 (Consejo de Protectores de 17 expertos independientes, Director Ejecutivo por procedimiento abierto, doble verificación humano-IA), como agencia sigue siendo **revocable por el legislador ordinario**:

Aspecto	EDSPA (agencia)	Poder Protector (4º poder)
Permanencia	Un reglamento puede derogarse por mayoría ordinaria	Solo reformable por el procedimiento del art. 48 TUE: Convención, unanimidad y ratificación por los 27
Autoridad	Poderes regulatorios y de supervisión dentro del acervo (DSA, AI Act, NIS2)	Poderes constitucionales propios: iniciativa legislativa, ejecución directa y acceso a jurisdicción especializada — Sala de Recurso administrativa (modelo ACER), Cámara Especializada en Protección Digital del Tribunal General y casación ante el TJUE (Cap. 12)
Ámbito	Los 9 Estados del núcleo fundador (art. 20 TUE) y las adhesiones posteriores	Todos los Estados Miembros, con efectos erga omnes
Financiación	Contribuciones anuales bajo el modelo 40/35/15/10 — sujeto a ciclos presupuestarios	Recursos propios: autonomía financiera garantizada por el Tratado
Independencia	Protegida por diseño (modelo ERC), pero políticamente reversible	Separación de poderes: imparcialidad por arquitectura constitucional
Adaptación	Requiere que el legislador actualice su mandato ante cada nueva amenaza	Mandato permanente sobre la esfera cognitiva, adaptable por derecho derivado propio

Nota de rigor: esta limitación no es un defecto de la EDSPA: es la razón por la que este libro la presenta siempre como *paso necesario* y nunca como solución final. El Capítulo 9 demostró su viabilidad económica (ROI 164% a 5 años en el escenario base, ~€2,6 devueltos por euro; beneficio neto +€1.820M/año a plena capacidad; equilibrio acumulado en 2028 según el Capítulo 9B). El valor de esa demostración no es que la agencia se quede ahí: es que hace defendible lo que viene.

11.3 El Poder Protector: la solución definitiva

Definición y propósito

El **Poder Protector** es el 4º poder constitucional: una institución permanente encargada de proteger la **esfera cognitiva** de los ciudadanos, las instituciones y la sociedad europea frente a la manipulación digital, garantizando que ningún actor — público o privado — pueda subvertir los procesos democráticos, la autonomía individual o la soberanía colectiva.

Por qué un 4º poder y no más de lo mismo

Poder tradicional	Función	Limitación frente a amenazas cognitivas
Ejecutivo	Implementa políticas	Sin experiencia especializada en protección cognitiva; dependiente de asesoramiento externo, frecuentemente influido por los intereses regulados
Legislativo	Crea leyes	Ciclos de varios años frente a amenazas que evolucionan en semanas; el acervo llega siempre tarde
Judicial	Interpreta leyes	Actúa sobre hechos consumados; no puede prevenir la manipulación algorítmica en curso

Ninguno de los tres tiene el mandato, la capacidad ni la agilidad para proteger la esfera cognitiva de forma **proactiva, integral y permanente**. El Poder Protector equilibra la asimetría estructural entre la tecnología (rápida, global, opaca) y la democracia (lenta, fragmentada, transparente) — igual que el Poder Judicial se creó para interpretar la ley con imparcialidad, el Poder Protector se crea para proteger la cognición con especialización.

Competencias exclusivas

Competencia	Descripción	Por qué ningún poder actual puede ejercerla
Protección cognitiva integral	Salvaguardar la esfera cognitiva de ciudadanos e instituciones	Requiere mandato específico, expertise dedicado y ejecución inmediata
Regulación algorítmica	Supervisar y auditar sistemas de IA y algoritmos	Exige conocimiento técnico especializado permanente, no consultoría puntual
Supervisión de plataformas	Auditar y requerir a las plataformas digitales	Necesita independencia absoluta frente a la captura corporativa
Protección electoral	Garantizar la integridad de los procesos democráticos	Demanda coordinación transnacional y acción preventiva, no reactiva
Derechos cognitivos	Tutelar libertad cognitiva, autonomía mental y privacidad	Los derechos digitales actuales están dispersos y carecen de garante institucional
Educación y resiliencia	Alfabetización digital y resiliencia social	Requiere enfoque pedagógico especializado y recursos dedicados sostenidos

11.4 Por qué no crear el Poder Protector directamente

La vía constitucional está codificada en el **artículo 48 TUE**: el procedimiento ordinario de revisión exige una **Convención**, una **conferencia intergubernamental**, la **unanimidad** del Consejo Europeo y la **ratificación por los 27** según sus normas constitucionales (en varios casos, referéndum). Las pasarelas del apartado 7 no sirven aquí: el derecho derivado no puede crear un nuevo poder constitucional.

La experiencia reciente confirma la dificultad: el Parlamento Europeo votó el **22 de noviembre de 2023** a favor de la reforma de los Tratados siguiendo la Conferencia sobre el Futuro de Europa, y pidió al Consejo Europeo que convocara la Convención — pero en el Consejo no se ha materializado el consenso para abrir el proceso. Las grandes revisiones históricas (del Acta Única a Lisboa) tardaron entre 4 y 8 años entre convocatoria y entrada en vigor. El horizonte más temprano defendible para un 4º poder constitucional es, por tanto, **2033**.

Obstáculo (hoy)	Solución EDSPA	Resultado
La reforma exige unanimidad y ratificación por los 27	Cooperación reforzada: solo 9 Estados (art. 20 TUE)	Arranque sin esperar consenso total
Falta de consenso político sobre la protección cognitiva	Los Estados dispuestos demuestran resultados tangibles	Los reticentes se suman por evidencia, no por coacción
Los ciudadanos no perciben la urgencia	Beneficios visibles: desinformación medida, confianza recuperada	Presión social para la reforma
No existe infraestructura, personal ni procesos	La EDSPA los construye y los depura	La reforma hereda capacidad, no promesas
Una reforma fallida debilitaría a la UE	Prueba de concepto antes de tocar el Tratado	Riesgo minimizado

La clave estratégica: el art. 20 TUE (cooperación reforzada) y el art. 48 TUE (revisión ordinaria) no son rivales: son *secuencia*. La cooperación reforzada es el único instrumento jurídico disponible hoy que permite actuar de inmediato contra la amenaza mientras se construye el consenso constitucional de mañana. Es exactamente el mecanismo con el que la UE ha avanzado históricamente cuando la unanimidad bloqueaba y la necesidad no podía esperar.

11.5 EDSPA como laboratorio: lo que la transición heredará

Activo	EDSPA (2026-2030)	Poder Protector (2033+)
Experiencia	Demuestra que la protección cognitiva funciona: métricas de detección, casos resueltos, auditorías algorítmicas	Aplica esa experiencia a escala constitucional
Capacidad	Construye herramientas, protocolos (doble verificación humano-IA), personal experto (1.500-2.000 empleados)	Hereda y escala esa capacidad operativa
Evidencia económica	ROI 164% a 5 años; beneficio neto + €1.820M/año a plena capacidad; equilibrio acumulado 2028 (Cap. 9B)	Convierte la viabilidad demostrada en argumento de reforma
Apoyo político	Los 9 fundadores generan un precedente de eficacia al que se suman más Estados	El consenso ampliado sostiene la ratificación
Apoyo ciudadano	Beneficios tangibles: menos desinformación, más confianza en el espacio digital	La presión social respalda el paso constitucional
Estándares	Normas técnicas, procedimientos de auditoría, estándares de protección electoral	Se institucionalizan en derecho constitucional y derivado propio
Base financiera	Presupuesto estabilizado en torno al escenario pleno (€1.000M/año)	Transfiere su capacidad presupuestaria como base inicial del Poder Protector, complementada por el régimen de recursos propios que desarrolla el Capítulo 16

11.6 El cronograma de la transición (2026-2035)

El cronograma alinea el doble escenario del Capítulo 10 con el procedimiento del art. 48 TUE. El punto de partida realista: el escenario acelerado sitúa la capacidad operativa inicial en **2028**, de modo que la propuesta de reforma puede presentarse sobre resultados — no sobre promesas — en **2028-2029**.

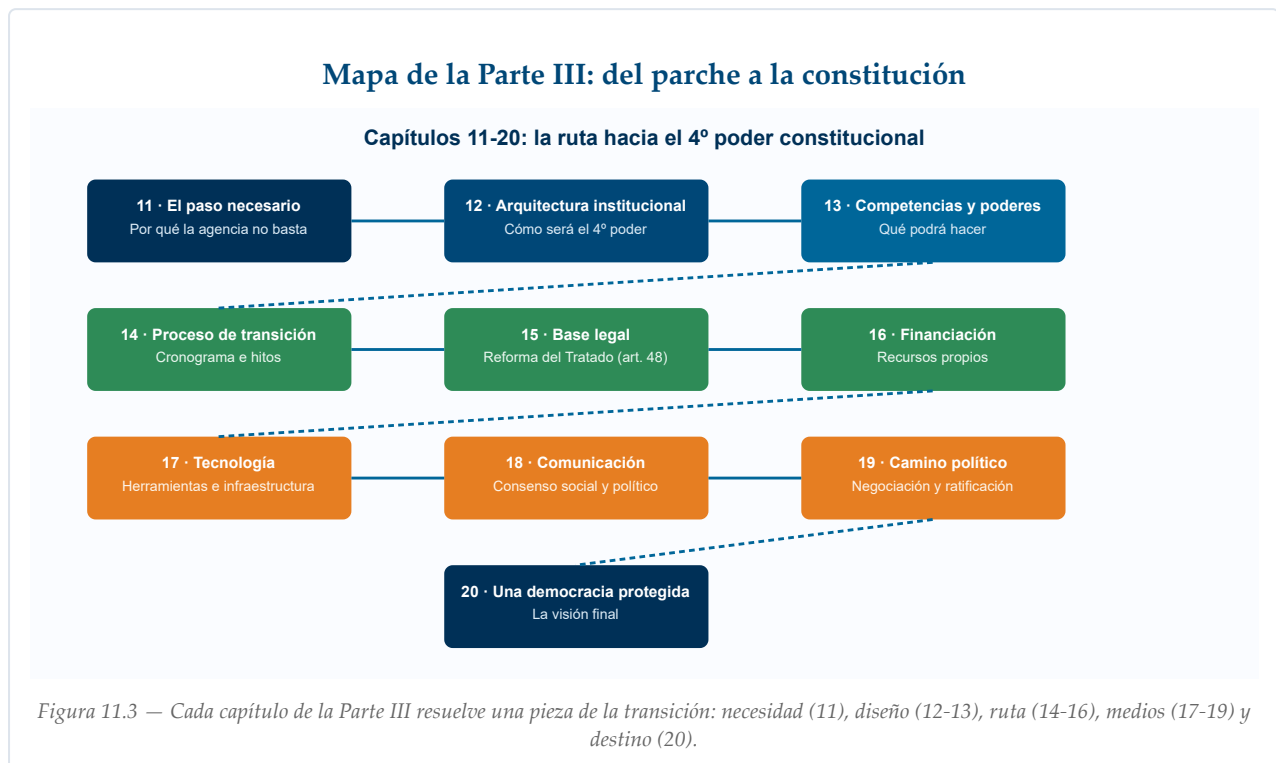
De la EDSPA al Poder Protector: 2026-2035



Figura 11.2 — Cronograma de transición: la EDSPA opera y demuestra resultados (2026-2029) mientras se abre el proceso constitucional (2029-2033) y se integran las estructuras (2033-2035).

Fase	Periodo	Objetivo	Indicador de éxito
1. Implementación EDSPA	2026-2028	Crear la agencia y alcanzar la capacidad operativa (escenario acelerado del Cap. 10)	EDSPA operativa con los 9 fundadores
2. Consolidación	2028-2029	Demostrar efectividad y acumular evidencia	Métricas de detección y caso de éxito público
3. Propuesta	2028-2029	Presentar la reforma constitucional sobre resultados	Consenso político inicial para abrir el proceso
4. Convención y CIG	2029-2032	Negociar la reforma del Tratado (art. 48 TUE)	Acuerdo unánime en el Consejo Europeo
5. Ratificación y vigor	2032-2033	Ratificación por los 27 según sus normas internas	Poder Protector en vigor en 2033
6. Integración	2033-2035	Transferir personal, herramientas, estándares y base presupuestaria de la EDSPA al Poder Protector	PP plenamente operativo; la EDSPA queda integrada

11.7 El hilo conductor de la Parte III (Capítulos 11-20)



11.8 Conclusión: la EDSPA es el medio; el Poder Protector es el fin

1. **La EDSPA es un paso necesario, pero insuficiente.** Como agencia, puede ser derogada, recortada o reorganizada por cualquier mayoría futura — como demuestran EDMO, EMSA y OLAF. Su valor no está en lo que logre por sí misma, sino en lo que permita construir.
2. **El Poder Protector es la solución definitiva.** Como 4º poder constitucional, sería permanente, especializado e imparcial por diseño: devolvería a las democracias el control sobre la esfera digital con la solidez que solo el derecho constitucional otorga.
3. **La EDSPA es el camino estratégico.** Demuestra que la protección cognitiva funciona, genera el apoyo político y social que la reforma exige, y deja construida la capacidad que el Poder Protector heredará. Actuar con los 9 hoy es lo que hace posible la unanimidad de los 27 mañana.

La continuidad del libro: la Parte I (Cap. 1-5) estableció el problema: las amenazas a la esfera cognitiva son existenciales para la democracia. La Parte II (Cap. 6-10) construyó el instrumento: la EDSPA, su diseño, su economía y su despliegue. La Parte III (Cap. 11-20) traza la ruta definitiva: del parche operativo de 2026 a la arquitectura constitucional de 2033.

11.9 Fuentes y referencias verificadas

- **Art. 48 TUE** (procedimientos ordinario y simplificado de revisión): EUR-Lex, texto consolidado del Tratado de la Unión Europea.
- **Art. 20 TUE y arts. 326-334 TFUE** (cooperación reforzada): EUR-Lex, textos consolidados.
- **Parlamento Europeo, 22 de noviembre de 2023:** resolución sobre las propuestas de modificación de los Tratados tras la Conferencia sobre el Futuro de Europa (solicitud de Convención).
- **EDMO:** página oficial de la Comisión Europea (digital-strategy.ec.europa.eu) y convocatorias DIGITAL sobre hubs con financiación «que termina en 2026».
- **EMSA:** propuesta COM(2023) 269 final, 1 de junio de 2023; acuerdo provisional Consejo-Parlamento, 20 de mayo de 2025 (Consejo de la UE).
- **OLAF:** Dictamen del Tribunal de Cuentas sobre la gestión de OLAF (EUR-Lex); investigación de Follow the Money sobre la dimensión no detectada del fraude (Fiscal Europeo de Cabeza).

- **Cifras económicas EDSPA:** Capítulos 9 y 9B de esta versión (ROI 164% a 5 años, beneficio neto +€1.820M/año, equilibrio acumulado 2028, núcleo de 9 Estados).

Capítulo 12: Arquitectura Institucional del Poder Protector

Resumen del capítulo

Este capítulo define la estructura completa del Poder Protector como 4º poder constitucional, sobre una decisión de diseño que lo atraviesa todo: **es un poder protector, no sancionador**. El PP no impone multas en ningún nivel — ni propio ni delegado —, no borra contenido y no decide qué se puede ver: su arma es la luz (detección, documentación probatoria, publicidad). Cuando la manipulación detectada exige respuesta coercitiva, el expediente se remite a quienes ya tienen la competencia sancionadora (la Comisión Europea bajo el DSA y el AI Act, con sus techos reales del 6% y 7%, o las autoridades nacionales) o se litiga ante los tribunales, con el PP como parte. La institución es **única** — no un holding de agencias — con un Consejo de Protección Cognitiva de modelo mixto (27 expertos independientes con voto y 27 representantes estatales con voz pero sin voto) y cuatro departamentos operativos bajo dirección ejecutiva única. El volumen de litigios técnicos que generará no se resuelve con un tribunal "propio" (que violaría la separación de poderes) sino con una **Cámara Especializada en Protección Digital dentro del Tribunal General**, del poder judicial y con presupuesto del poder judicial, con jueces de doble cualificación (modelo del Tribunal Unificado de Patentes) y cláusula de escalado. La EDSPA se integra como embrión del Departamento de Protección Cognitiva. Marco económico: el del Cap. 17 — **€2.600M/año base / €3.400M pleno**, con recursos propios (Cap. 16). Y la dotación de personal es la de un poder, no la de una agencia: una trayectoria por etapas que va de los 1.500-2.000 heredados de la EDSPA a **más de 15.000 efectivos en la madurez 2040+** (Cap. 15) — con una proporción creciente deliberadamente no automatizable: el mayor polo europeo de empleo público del juicio humano.

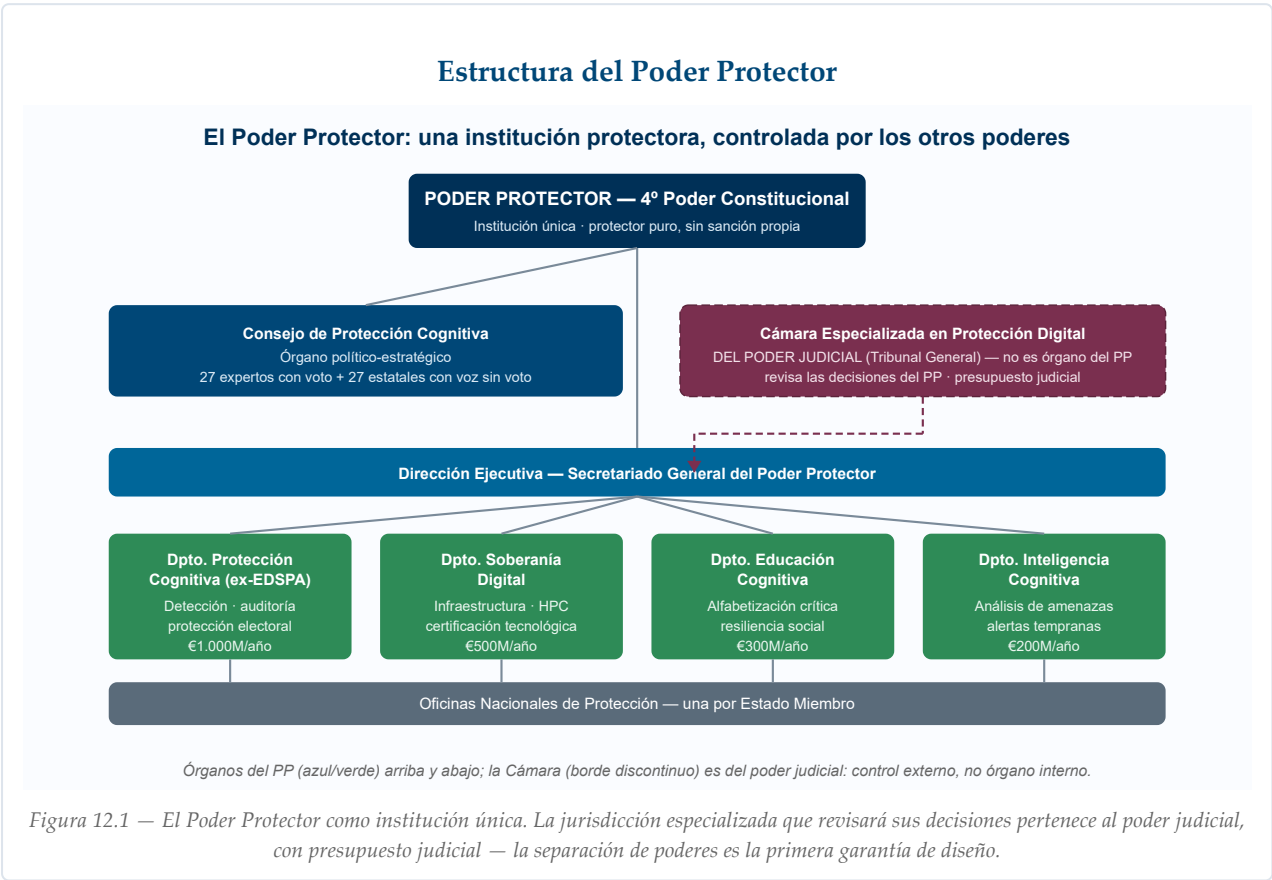
12.1 Principios fundamentales de diseño

Principio	Descripción	Aplicación práctica
Protección, no sanción	El PP detecta, documenta y expone; nunca castiga ni censura	Las sanciones corresponden a las autoridades existentes (Comisión, Estados) y a los jueces; el PP es parte procesal, no juez
Separación de poderes	Independencia absoluta frente a Ejecutivo, Legislativo y Judicial — y de ellos	Prohibición expresa de injerencias mutuas; el PP no absorbe funciones judiciales ni sancionadoras de otros poderes
Especialización	Foco exclusivo en la esfera cognitiva digital	No puede asumir competencias de otros poderes; mandato delimitado por el Tratado
Omnipresencia	Cobertura total: todos los Estados Miembros, todas las plataformas	Jurisdicción de detección y auditoría en toda la UE con efectos erga omnes
Inalterabilidad	Solo reformable con unanimidad (art. 48 TUE)	Protección constitucional contra cambios políticos coyunturales
Transparencia radical	Rendición de cuentas ante ciudadanos e instituciones	Auditorías externas obligatorias (Tribunal de Cuentas), informes públicos anuales y acceso documental estructural

Por qué "protector puro" y no "protector sancionador" (conexión con el Cap. 11): el Capítulo 11 estableció que el PP debe ser permanente e inalterable. Pero un poder permanente *con* capacidad sancionadora propia y sin control interno sería percibido — con razón — como un riesgo para las libertades, y esa percepción bastaría para hundir la ratificación. La solución no es menos poder: es un poder distinto. El PP concentra en su nivel constitucional lo que las instituciones actuales no pueden hacer (detección sistemática, auditoría algorítmica continua, publicidad probatoria) y deja intacta la coerción en manos de quienes ya la ejercen bajo control judicial pleno. **Ningún actor decide qué se puede ver; todos pueden saber quién está intentando manipularlos.**

12.2 El organigrama: una institución única con departamentos

La experiencia europea con estructuras fragmentadas de agencias (el paisaje revisado en los Capítulos 6 y 11) recomienda lo contrario: **una sola institución con dirección única**, cuyas funciones operativas se organizan como departamentos internos. Esto elimina solapes y hace imposible el juego de «agencia contra agencia». La dimensión judicial no es un órgano del PP: pertenece al poder judicial de la UE (sección 12.4).



12.3 El Consejo de Protección Cognitiva

El Consejo es el órgano político-estratégico del Poder Protector. Su diseño resuelve la tensión entre la **imparcialidad técnica** que exige un poder que vigila la manipulación y la **legitimidad política** sin la cual la reforma del Tratado no será ratificada. La solución es un **modelo mixto con voto desigual**:

Miembros	Número	Selección	Mandato	Poder de decisión
Expertos independientes	27 (uno por Estado Miembro en representación geográfica, elegidos por mérito)	Convocatoria pública paneuropea + evaluación técnica + lista corta + sorteo público (modelo ERC del Cap. 7, ampliado de 17 a 27)	8 años, no renovable, mandato escalonado	Voto — única cámara con capacidad de decisión
Representantes estatales	27 (uno por Estado Miembro)	Designados por los gobiernos nacionales	4 años, revocables por su gobierno	Voz pero sin voto — información, deliberación y capacidad de impugnar ante la jurisdicción especializada
Presidencia	1	Elegida por el Pleno entre los expertos independientes	5 años, no renovable	Dirige y representa al Consejo

Mecanismo de selección de los expertos (mérito + sorteo)

1. **Convocatoria pública** en toda la UE, con criterios de elegibilidad públicos.
2. **Evaluación por comité independiente** según el estándar del Consejo Europeo de Investigación.
3. **Lista corta** con al menos el triple de posiciones por Estado Miembro.

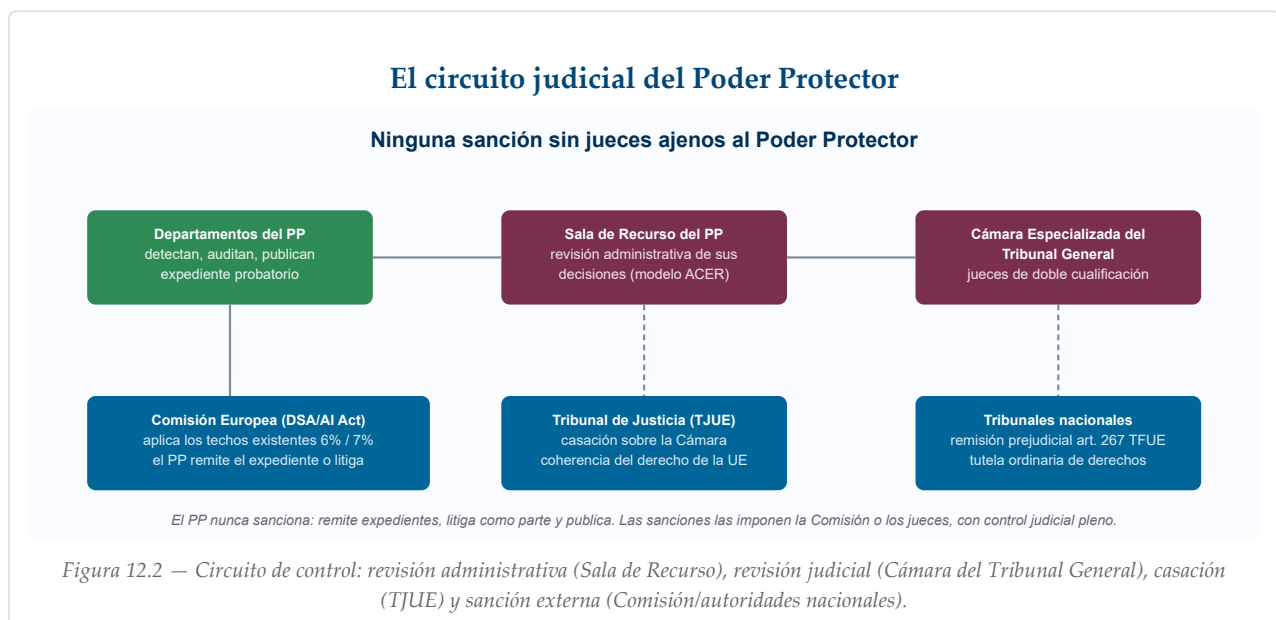
4. **Sorteo público** auditado ante la Oficina de Publicaciones, notarios y medios.
5. **Ratificación** por el Pleno salvo inelegibilidad sobrevenida.

Funciones del Consejo

- **Iniciativa legislativa** en materia de protección cognitiva: el PP propone; el Parlamento y el Consejo de la UE deciden con el procedimiento legislativo ordinario.
- **Dirección estratégica**: prioridades, reglamento interno, planes plurianuales.
- **Supervisión de los departamentos** a través de la Dirección Ejecutiva.
- **Coordinación interinstitucional** con Ejecutivo, Legislativo y Judicial y con los Estados Miembros.

12.4 El encaje judicial: jurisdicción especializada dentro del poder judicial

El PP generará un volumen significativo de litigios técnicos — auditorías algorítmicas impugnadas, recursos contra sus decisiones operativas, conflictos entre plataformas y derechos cognitivos. La tentación de resolverlo con un "Tribunal de Protección Digital" propio del PP fue descartada en esta versión: **un tribunal dentro de un poder viola la separación de poderes y confirmaría la percepción de un poder juez y parte**. La solución viable, avalada por los precedentes reales, tiene tres piezas:



a) La Sala de Recurso administrativa (primera garantía, modelo ACER)

Las decisiones operativas del PP (resultados de auditoría, designaciones de plataformas vigiladas, requerimientos de información) serán recurribles ante una **Sala de Recurso** interna pero independiente, siguiendo el modelo verificado de las Salas de Recurso de las agencias de la UE (ACER, CPDP): revisión *plena* de la decisión impugnada, con peritos técnicos, apelable ante el Tribunal General. La jurisprudencia del TJUE (Aquind c. ACER, C-46/21 P) valida estas salas como mecanismo apropiado de protección de derechos en decisiones técnicas complejas.

b) La Cámara Especializada en Protección Digital (segunda garantía, dentro del poder judicial)

El volumen y la tecnicidad de los litigios justifican especialización, no un tribunal nuevo. La propuesta: una **Cámara Especializada en Protección Digital del Tribunal General**, creada por reglamento ordinario (sin reforma del Tratado), con:

Elemento	Diseño	Precedente verificado
Naturaleza	Cámara del Tribunal General: pertenece al poder judicial, con presupuesto judicial — no al PP	Salas especializadas internas (modelo IP High Court de Tokio, IPEC británico)
Jueces	Formación dual acreditada: derecho + ciencia/tecnología, con pool permanente de referendarios técnicos	Tribunal Unificado de Patentes: 34 jueces jurídicos + 51 técnicos
Creación	Reglamento ordinario (art. 257 TFUE permite además tribunales especializados si el volumen lo exige)	Sistema del art. 19 TUE
Cláusula de escalado	Si la Cámara supera de forma sostenida el umbral de carga (referencia orientativa: 150-200 asuntos/año), se activa el tribunal especializado del art. 257 — solo por demanda real	Lección del Tribunal de la Función Pública: creado en 2004, suprimido en 2016 por falta de volumen
Control	Casación ante el Tribunal de Justicia; cuestiones prejudiciales (art. 267 TFUE) para la coherencia con los tribunales nacionales	Art. 19 TUE y Estatuto del TJUE

Por qué no un tribunal propio del PP: el precedente más cercano desaconseja además la creación prematura de tribunales: el Tribunal de la Función Pública (creado en 2004, 7 jueces) fue **suprimido en 2016** y su competencia devuelta al Tribunal General, porque su volumen de asuntos no justificaba la estructura fija. Y cuando el sistema judicial de la UE se ha saturado de verdad, la respuesta ha sido ampliar lo existente — el Tribunal General duplicó sus jueces de 28 a 56 entre 2016 y 2019 para eliminar su atasco — no crear instituciones paralelas. La Cámara especializada con escalado condicionado sigue ambas lecciones: especialización real, estructura proporcional a la demanda.

c) La sanción: siempre externa, siempre judicialmente controlable

El PP no tiene techos sancionadores propios. Los techos reales ya existen en el acervo: **hasta el 6% de la facturación mundial (DSA) y hasta el 7% o €35M (AI Act)**. Lo que falta hoy no son techos mayores: es detección sistemática y litigio efectivo. La contribución del PP es exactamente eso:

- **Remisión de expedientes probatorios** a la Comisión Europea y a las autoridades nacionales competentes, con estándar de prueba judicial desde el primer día.
- **Litigio como parte** ante la Cámara Especializada y, vía prejudicial, ante los tribunales nacionales.
- **Publicidad:** la manipulación documentada se publica — el coste reputacional y de mercado es, en la mayoría de los casos, la sanción más inmediata.

Nota de rigor: la separación entre detectar y sancionar, establecida para la EDSPA en los Capítulos 6-9, queda así elevada a la arquitectura misma del 4º poder y simplificada al máximo: **el PP no toca la sanción ni el dinero de las multas en ningún nivel**. La recaudación de las sanciones es siempre presupuesto general de la UE. Esta simplificación eliminó también el "Comité de Sanciones" y el "Tribunal de Protección Digital" de diseño inicial.

12.5 Los departamentos operativos

Departamento	Función	Presupuesto/año	Notas de diseño
Protección Cognitiva (ex-EDSPA)	Detección de manipulación, auditoría algorítmica, protección electoral, supervisión de plataformas	€1.000M	Hereda íntegramente la capacidad de la EDSPA: protocolos de doble verificación humano-IA, personal experto, estándares
Soberanía Digital	Independencia tecnológica: capacidad de cómputo europea (EuroHPC y sucesores), certificación tecnológica, control de datos estratégicos	€500M	Arranca donde el Cap. 17 sitúa los datacenters propios del Poder Protector
Educación Cognitiva	Alfabetización digital crítica, formación de periodistas y educadores, campañas, investigación en manipulación	€300M	Objetivo propio: ≥90% de alfabetización crítica digital para 2038 , superando el objetivo de la Década Digital (80% en 2030)
Inteligencia Cognitiva	Análisis de amenazas emergentes, patrones de desinformación, alertas tempranas, coordinación con servicios nacionales	€200M	Garantías: supervisión de la Sala de Recurso y de la Cámara, informe público anual, auditorías del Parlamento Europeo
Suma departamentos	Función operativa del Poder Protector	€2.000M	Más Consejo, Dirección Ejecutiva, Sala de Recurso y Oficinas Nacionales → marco del Cap. 17
Marco total del Poder Protector	Institución completa	€2.600M base / €3.400M pleno	Recursos propios (Cap. 16). La Cámara Especializada se financia con cargo al presupuesto del poder judicial de la UE, no del PP

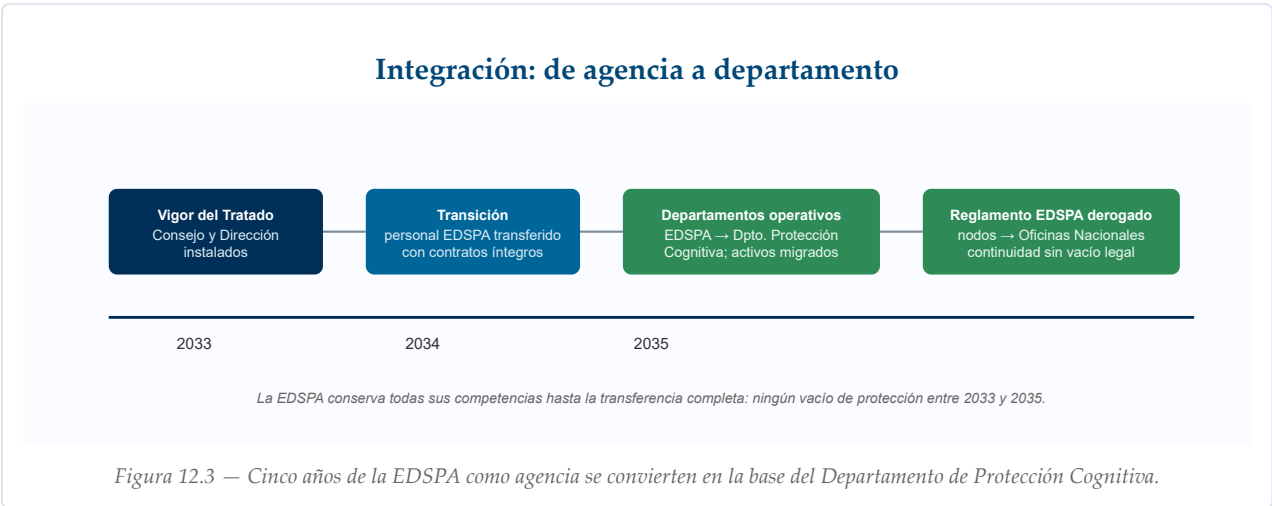
Cifras reales de contexto: el objetivo de alfabetización se ancla en el objetivo oficial de la Década Digital de la UE — **80% de adultos con competencias digitales básicas en 2030** — frente al ~55,6% verificado a mediados de la década. El objetivo propio del PP (≥90% en 2038) es estimación de diseño de este libro, etiquetada como tal. Dimensionamiento judicial asociado (estimación propia, cargada al presupuesto judicial): Cámara de 7-9 jueces duales con ~4 referendarios cada uno y pool de peritos, en el orden de €40-60M/año — comparable al coste real por juez del sistema TJUE.

Dotación de personal — trayectoria, no plantilla: los departamentos no nacen con su dotación de madurez: crecen por etapas con disparadores contables (adhesiones de Estados, cobertura de la misión, volumen de amenaza, ampliaciones autorizadas por el legislador), como le ha ocurrido a todo poder europeo — la Comisión de unos pocos miles a ~32.000; Frontex de decenas de analistas a un cuerpo estatutario de 10.000 para 2027. La trayectoria completa (1.500-2.000 EDSPA → ~3.000 núcleo → ~7.000-8.000 pleno ~2037 → **>15.000 madurez 2040+**) se fundamenta en el Cap. 15. El límite que no escala es el de naturaleza: los cometidos de cada departamento están congelados por el protector puro del Cap. 13. Y una proporción creciente de esa plantilla es deliberadamente no automatizable: la doble verificación humano-IA del Cap. 8 hace del PP el mayor empleador público europeo del juicio humano no automatizable frente a la IA.

12.6 Las Oficinas Nacionales

Elemento	Diseño
Presencia	1 oficina por Estado Miembro (27), tamaño proporcional a la población y a la exposición a amenazas
Función	Implementación territorial, coordinación con autoridades nacionales, quejas ciudadanas, monitoreo local, educación
Relación con los nodos EDSPA	Los nodos nacionales de la EDSPA (Cap. 7) son el embrión directo: se transforman en Oficinas Nacionales al completarse la integración
Financiación	Con cargo al presupuesto del Poder Protector (recursos propios), sin cofinanciación estatal que comprometa la independencia

12.7 La integración de la EDSPA (2033-2035)



Aspecto	EDSPA como agencia (2026-2035)	Dpto. de Protección Cognitiva en el PP (2035+)
Base legal	Reglamento de cooperación reforzada (art. 20 TUE)	Tratado de la UE: competencia constitucional
Autoridad	Regulatoria, dentro del acervo (DSA, AI Act, NIS2)	Constitucional: iniciativa legislativa y ejecución propia de protección
Ámbito	Estados participantes (los 9 fundadores y adhesiones)	Los 27, con efectos erga omnes
Financiación	Modelo 40/35/15/10, ciclo presupuestario anual	Recursos propios (Cap. 16): autonomía financiera constitucional
Sanción	Remisión a las autoridades competentes	Remisión y litigio: el PP sigue sin sancionar — la sanción es externa y judicialmente controlable (sección 12.4)
Control judicial	Tribunales de la UE y nacionales	Sala de Recurso + Cámara Especializada del Tribunal General + casación TJUE
Personal	1.500 (base) a 2.000 (acelerado) empleados	Transferidos íntegramente + trayectoria de dotación por etapas (Cap. 15): ~3.000 en el núcleo 2033-2035 → ~7.000-8.000 en el pleno ~2037 (27 Estados, 24 lenguas, 24/7) → >15.000 en la madurez 2040+

Garantías de continuidad: transferencia automática de contratos; operación ininterrumpida de la EDSPA hasta la derogación de su reglamento; migración de datos validada por ENISA; mantenimiento de todas las competencias hasta el último día (sin vacío legal); presupuesto del PP garantizado desde el primer día del vigor del Tratado.

12.8 Comparativa: la agencia frente al poder constitucional

Qué cambia con la integración

De la agencia (revocable) al 4º poder (constitucional) — sin tocar la sanción

EDSPA: reglamento derogable por mayoría
jurisdicción solo en Estados participantes

Sanción siempre externa, control judicial general
presupuesto anual negociado (40/35/15/10)

Poder Protector: solo reformable por unanimidad
jurisdicción de protección en los 27

Sanción externa con jurisdicción especializada propia
recursos propios: autonomía financiera

La protección cognitiva pasa de decisión política anual a compromiso constitucional permanente.

Lo que no cambia: la sanción sigue fuera del poder protector, en manos de la Comisión y de los jueces.

Figura 12.4 — Las mejoras de la integración: permanencia, cobertura universal, jurisdicción especializada y autonomía financiera. La separación detectar/sancionar es lo único que se conserva idéntico.

12.9 Conclusión: la arquitectura de un poder para el siglo XXI

1. **El Poder Protector será una institución única y protectora**, no sancionadora: Consejo mixto con voto técnico, dirección ejecutiva única, cuatro departamentos operativos y capilaridad nacional. Su arma es la luz: detección probatoria, auditoría continua y publicidad.
2. **La sanción queda íntegramente fuera del PP**: los techos existentes (DSA 6% / AI Act 7%) los aplican la Comisión y las autoridades nacionales; el PP remite expedientes y litiga como parte. Ningún tribunal propio, ningún comité sancionador, ningún dinero de multas.
3. **El volumen judicial se resuelve dentro del poder judicial**: Sala de Recurso administrativa (modelo ACER), Cámara Especializada del Tribunal General con jueces de doble cualificación (modelo UPC) y cláusula de escalado condicionado a la demanda real (lección del Tribunal de la Función Pública).
4. **La EDSPA no desaparece: se integra** como Departamento de Protección Cognitiva, heredando personal (1.500-2.000 empleados), herramientas, estándares y base presupuestaria (€1.000M/año), sin dejar ni un día de protección entre 2033 y 2035. Y desde ahí arranca la trayectoria de dotación de un poder (Cap. 15): ~3.000 efectivos en el núcleo 2033-2035 → ~7.000-8.000 en el pleno ~2037 → más de 15.000 en la madurez 2040+.

La tesis del capítulo en una frase: el Poder Protector no castiga la manipulación — la hace visible. Y la visibilidad, con jueces independientes y autoridades sancionadoras existentes detrás, es más eficaz y más segura para las libertades que cualquier multa impuesta por un poder juez y parte.

12.10 Fuentes y referencias verificadas

- **Art. 19 TUE** (sistema judicial), **art. 257 TFUE** (tribunales especializados) y **art. 267 TFUE** (prejudicial): EUR-Lex, textos consolidados.
- **Precedente de tribunales especializados**: Tribunal de la Función Pública de la UE (2004-2016), suprimido por el Reg. (UE, Euratom) 2016/1192 y reintegrado en el Tribunal General.
- **Ampliación del Tribunal General**: duplicación de 28 a 56 jueces (2016-2019) para eliminar el atasco; estadísticas 2024 del TJUE (1.706 asuntos nuevos, 1.785 resueltos, 2.508 pendientes).
- **Salas de Recurso de agencias**: modelo ACER/CPDP; TJEU, Aquind c. ACER, C-46/21 P (revisión plena de decisiones técnicas complejas).
- **Jueces de doble cualificación**: Tribunal Unificado de Patentes (34 jueces jurídicos + 51 técnicos, 2022).
- **Techos sancionadores del acervo**: DSA (Reg. 2022/2065, hasta 6% de la facturación mundial) y AI Act (Reg. 2024/1689, hasta 7% o €35M).
- **Década Digital de la UE**: objetivo del 80% de adultos con competencias digitales básicas en 2030 (Decisión 2022/2481); cobertura verificada ~55,6% (Comisión Europea, JRC).

- **Ecosistema europeo de IA:** Mistral AI, Aleph Alpha, Apertus; fondo InvestAI (€200.000M) y fábricas de IA de EuroHPC.
- **Marco económico:** Capítulo 17 (€2.600M base / €3.400M pleno) y recursos propios del Capítulo 16.

Capítulo 13: Competencias del Poder Protector

Resumen del capítulo

Este capítulo define las competencias exclusivas del Poder Protector. La tesis es una **no se trata de crear un poder nuevo, sino de transferir el control de la esfera cognitiva desde actores no democráticos a instituciones públicas** reconstruida aquí sobre la decisión de diseño consagrada en el Capítulo 12: el PP es un **poder protector puro**. Sus competencias se agrupan en cinco verbos — **detectar, auditar, publicar, remitir y educar** — y están rodeadas de límites explícitos tan importantes como las propias competencias: el PP no sanciona (los expedientes van a la Comisión bajo el DSA y el AI Act, o a las autoridades nacionales), no elimina ni filtra contenido, no sustituye a las plataformas en la distribución y jamás decide qué información es «relevante». Su inteligencia artificial propia no es un árbitro de la verdad: es un **escáner forense cognitivo** que detecta patrones de manipulación y genera evidencia auditable bajo doble verificación humana. El capítulo sitúa estas competencias en el contexto regulatorio real de 2025-2026 — un acervo europeo considerable (DSA, AI Act, Data Act, Paquete de Soberanía Tecnológica, Escudo Europeo de la Democracia) al que le falta exactamente lo que el PP aporta: un ejecutor sistemático — y cierra con la previsión, en tres fases y sin compromiso presupuestario, del **Comprobador Ciudadano**, un servicio público de verificación no vinculante concebido como herramienta de educación digital.

13.1 El vacío de poder digital: quién controla la esfera cognitiva hoy

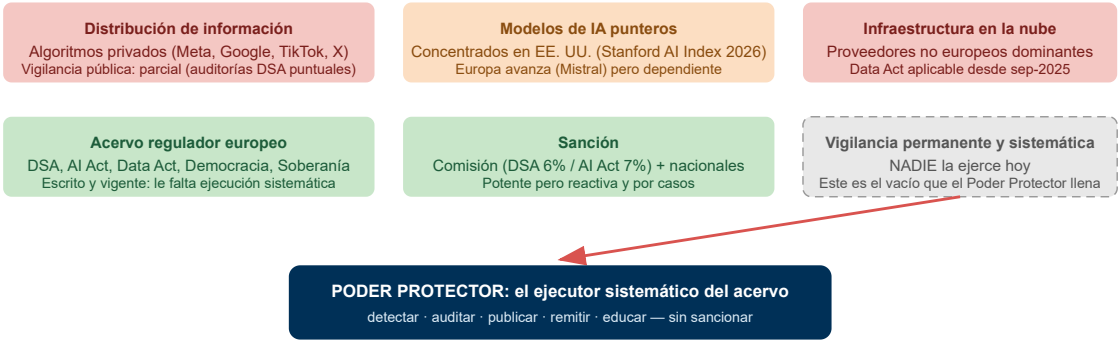
El control efectivo de la esfera cognitiva está en manos de actores que no responden ante los ciudadanos. Esta sección lo documenta solo con lo que las fuentes reales sostienen:

- **Exposición a la desinformación:** el Eurobarómetro de febrero de 2025 encontró que un **36% de los europeos** declara estar expuesto «a menudo» o «muy a menudo» a contenidos que considera distorsionados o falsos. No es una mayoría, pero es más de un tercio de la población expuesta de forma habitual.
- **Erosión de la confianza informativa:** el *Digital News Report* del Reuters Institute (edición 2026) documenta una caída continuada de la confianza en las noticias, el auge de los creadores individuales como fuente y el crecimiento del consumo informativo mediado por asistentes de IA — un ecosistema donde la distribución la deciden cada vez más sistemas opacos.
- **Dependencia tecnológica:** el Stanford AI Index (2026) confirma que los **Estados Unidos concentran la producción de los modelos de IA punteros** y China lidera en publicaciones científicas, mientras Europa avanza con actores propios (Mistral) pero desde una posición de dependencia. No existe un «90%» verificable, pero la asimetría estructural es real y medida.
- **Manipulación de origen mixto:** los estudios del Observatorio Europeo de los Medios Digitales (EDMO) y el tercer informe FIMI del Servicio Europeo de Acción Exterior muestran que las campañas de manipulación informativa en Europa combinan **actores domésticos y extranjeros** — no hay un «60% de origen externo» verificable, y la amenaza no es solo geopolítica: es también endógena.

La reformulación honesta del vacío

No sabemos con precisión estadística qué porcentaje del poder digital controlan los actores privados y hostiles. Sí sabemos tres cosas verificadas: **(1)** que los sistemas de distribución de la información que usan cientos de millones de europeos son privados y opacos; **(2)** que más de un tercio de los ciudadanos se percibe expuesto de forma habitual a desinformación; y **(3)** que ninguna institución pública europea tiene hoy el mandato permanente y sistemático de mirar dentro de esos sistemas. Ese es el vacío: no una conspiración, una **ausencia de vigilancia democrática**.

El vacío de poder digital: quién controla qué en la esfera cognitiva (2026)



El vacío de poder en datos reales:
36% expuesto a menudo a desinformación (Eurobarómetro feb-2025) ·
confianza informativa en caída (Reuters DNR 2026) · manipulación doméstica y extranjera (EDMO, EEAS FIMI)

El vacío no es «la mayoría del poder en manos privadas»: es la ausencia de una institución pública que mire de forma permanente.

Figura 13.1 — Mapa del vacío de poder digital: el acervo existe, la sanción existe, la vigilancia sistemática no existe. El Poder Protector no sustituye a nadie: ocupa un espacio vacío.

13.2 El marco de competencias: cinco verbos y sus límites

Las competencias se organizan bajo el principio de protección pura: Áreas de actuación descritas como **funciones de protección** con límites explícitos y ninguna función sancionadora.

Competencia	Qué hace el Poder Protector	Quién la ejerce hoy	Límite explícito (lo que el PP nunca hará)
Detectar	Escanear la esfera cognitiva con la IA forense propia y con equipos humanos para identificar campañas de manipulación, coordinación inauténtica y vulneraciones de derechos cognitivos	Plataformas (interés propio, opaco), hubs EDMO (limitados y por proyecto), ningún actor público sistemático	No etiqueta contenido como «verdadero» o «falso» para el público; genera indicios y evidencia interna con doble verificación
Auditar	Auditar algoritmos, sistemas de recomendación, sistemas de IA y prácticas de datos conforme al DSA (art. 40: acceso a datos), el AI Act y el Data Act	Comisión y DSCs nacionales (por casos, capacidad limitada); el acto delegado del art. 40 DSA (jul-2025) organiza el acceso de investigadores, no una auditoría pública sistemática	No aprueba ni veto cambios algorítmicos: audita y publica lo que ve; la decisión sigue siendo de la plataforma bajo el acervo
Publicar	Difundir informes de auditoría, registros de manipulación detectada y transparencia algorítmica — el arma del PP es la luz	Nadie de forma sistemática: los datos de auditoría DSA son confidenciales por defecto	No publica datos personales ni contenido privado; publica hallazgos agregados con respeto al secreto comercial legítimo
Remitir	Enviar expedientes probatorios a quien tiene la competencia sancionadora: Comisión Europea (DSA 6% / AI Act 7%), autoridades nacionales de mercado, y litigar como parte ante la jurisdicción especializada (Cap. 12)	La sanción ya existe y es ajena al PP; lo que falta es el alimentador sistemático de expedientes	No impone ni una multa, ni siquiera delegada; no se apropia del expediente: lo remite y hace seguimiento público
Educar	Alfabetización cognitiva (Departamento de Educación Cognitiva, €300M/año, meta ≥90% en 2038 anclada a la Década Digital), formación de periodistas, investigación aplicada	Estados (descoordinado), ONGs y EDMO (recursos limitados)	No impone currículo doctrinal: competencias verificables de detección de manipulación, sin sesgo ideológico, auditado (Cap. 8)

13.3 El escáner forense cognitivo: la IA del Poder Protector

El error más peligroso posible sería convertir a la IA del Poder Protector en árbitro de la relevancia: un Estado con un algoritmo que decide qué información es relevante sería exactamente el sistema de censura computacional que el propio libro denuncia — solo que con otro dueño. El diseño lo impide con una pieza central:

Qué es — y qué no es — la IA del Poder Protector

Es: un **escáner forense cognitivo**. Detecta patrones estadísticos de manipulación — coordinación inauténtica, redes de amplificación, deepfakes, operaciones FIMI, explotación algorítmica — y genera **evidencia auditable**: registros, linajes de datos, cadenas de custodia digital. Cada hallazgo pasa por el protocolo de **doble verificación humano-IA** del Capítulo 8 antes de convertirse en expediente. La IA es un instrumento forense, como el laboratorio de una policía científica: detecta indicios, no verdades.

No es: un árbitro del contenido. El escáner **nunca rankea, filtra, prioriza ni bloquea** información. Los algoritmos de las plataformas siguen decidiendo la distribución — bajo el acervo europeo y auditados por el PP. El poder de quién ve qué no se traslada a Bruselas: se somete a la luz. Cuando el escáner encuentra algo grave, el resultado no es un borrado: es un expediente, una publicidad y, si procede, una remisión a la Comisión o un litigio ante la Cámara Especializada.

Esta distinción es la que separa al Poder Protector de cualquier ministerio de la verdad. Un poder que filtra es un censor con mejor branding. Un poder que detecta, documenta y publica es un **constructor de evidencia pública**: cambia el debate no porque controle lo que se ve, sino porque ya nadie puede manipular a oscuras sin que quede constancia.

13.4 El Comprobador Ciudadano: verificación no vinculante como educación digital

Dar a la ciudadanía acceso directo a capacidad de verificación es una intuición valiosa. Desarrollada sin cuidado, sería peligrosa: un «verificador oficial» que dictaminara verdades sería un oráculo estatal. En su forma refinada, se convierte en una pieza coherente con el protector puro: el **Comprobador Ciudadano**, definido con precisión normativa:

- **Naturaleza:** servicio público de verificación **no vinculante y sin valor judicial**. El ciudadano pega un contenido (enlace, texto, imagen, vídeo) y recibe un informe **privado de indicios**: técnicas de manipulación detectadas, señales forenses (síntesis de imagen, coordinación de amplificación), contexto verificable. El informe no emite etiquetas de «verdadero» o «falso»: la conclusión es siempre del ciudadano.
- **Aviso permanente:** cada informe lleva incorporada la advertencia de que no es dictamen, no tiene valor probatorio y no sustituye el juicio propio. El Comprobador es una herramienta de alfabetización con formato de herramienta, no un juez con interfaz web.
- **Privacidad por diseño:** acceso autenticado vía eIDAS, pero consultas **pseudonimizadas sin vínculo reversible** con la identidad; retención mínima bajo supervisión del EDPS; las consultas no se comunican jamás a terceros, no generan expedientes y no alimentan remisiones. Lo que un ciudadano comprueba es irrelevante para el PP: solo importa que aprenda a comprobar.
- **Simetría anti-arma:** el escáner forense es el mismo para todos los contenidos — incluidos los del propio Poder Protector, los comunicados oficiales y las campañas electorales. Un instrumento que solo verifica a los demás es un arma; uno que también verifica al poder es un espejo.
- **Riesgos reconocidos:** el Comprobador puede ser capturado mediáticamente («el informe dice que...») o generar confianza excesiva en sustitución del criterio propio. Las mitigaciones son el formato de indicios (nunca veredictos), el aviso permanente y, sobre todo, la alfabetización: el objetivo del servicio es volverse innecesario.

Implementación escalonada: solo una previsión, no un compromiso

Fase 1 — EDSPA (2027-2030): no existe servicio ciudadano. Solo la IA forense interna, usada para vigilancia de la esfera cognitiva y expedientes.

Fase 2 — Poder Protector (2033-2035): estudio de viabilidad y auditoría de diseño (impacto en privacidad ante el EDPS, diseño técnico ante la Sala de Recurso). Sin fecha ni presupuesto comprometidos.

Fase 3 — Evaluación favorable (~2036+): lanzamiento gradual — primero piloto con investigadores acreditados y verificación externa de tasas de error; luego apertura progresiva a la ciudadanía, solo si el balance riesgo/beneficio es favorable y está documentado.

El Capítulo 13 **prevé** el Comprobador: no lo promete ni lo presupuesta. Si la evaluación es negativa, el PP funciona igual de completo sin él.

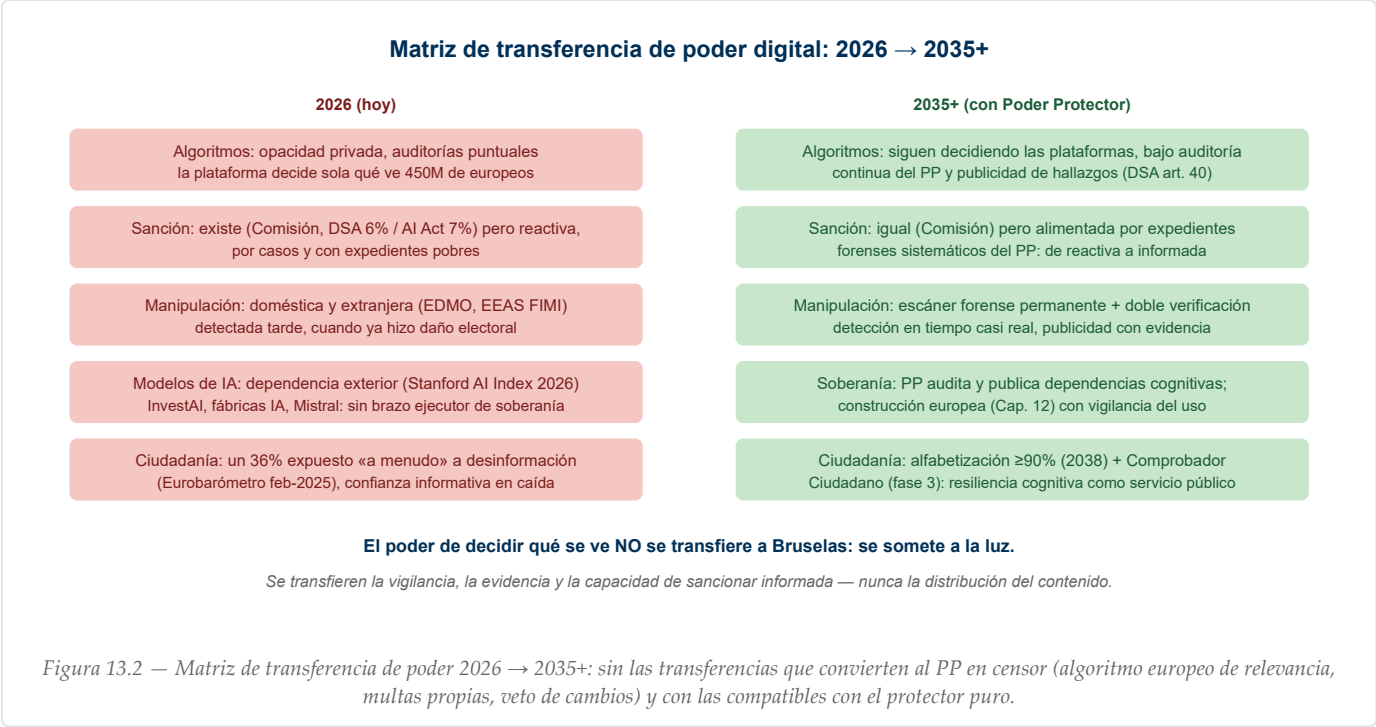
13.5 El contexto regulatorio real: por qué el acervo necesita un ejecutor

La urgencia se ancla en el calendario regulatorio real, verificable en el Diario Oficial de la UE:

Instrumento	Estado (verificado)	Lo que aporta	Lo que le falta
DSA (Reg. 2022/2065)	Vigente; acto delegado del art. 40 sobre acceso de investigadores a datos adoptado en julio de 2025	Transparencia algorítmica, auditorías, techos sancionadores del 6%, acceso a datos	El acceso se organiza por casos y por investigadores acreditados: no hay vigilancia pública sistemática y continua de la esfera cognitiva
AI Act (Reg. 2024/1689)	Aplicabilidad plena el 2 de agosto de 2026	Obligaciones por niveles de riesgo, techos del 7%, vigilancia de sistemas de IA	Enfoque por producto, no por esfera: nadie vigila el efecto agregado de los sistemas de IA sobre la cognición colectiva
Data Act (Reg. 2023/2854)	Aplicable desde el 12 de septiembre de 2025	Interoperabilidad, cambio de proveedor, acceso a datos de dispositivos	Regula la circulación de datos, no quién los usa para manipular la esfera cognitiva
Escudo Europeo de la Democracia	Presentado por la Comisión el 12 de noviembre de 2025	Respuesta a la interferencia extranjera, en línea con la Recomendación (UE) 2023/2829 sobre procesos electorales inclusivos y resilientes (2023)	Enfoque de seguridad y ciberdefensa, centrado en actores extranjeros: la manipulación doméstica y algorítmica queda fuera de su foco
Paquete de Soberanía Tecnológica	Presentado el 3 de junio de 2026	Cloud and AI Development Act y Cloud Sovereignty Framework: infraestructuras cloud europeas, reducción de dependencias	Construye soberanía de medios, pero no protege la esfera cognitiva de cómo se usan esos medios

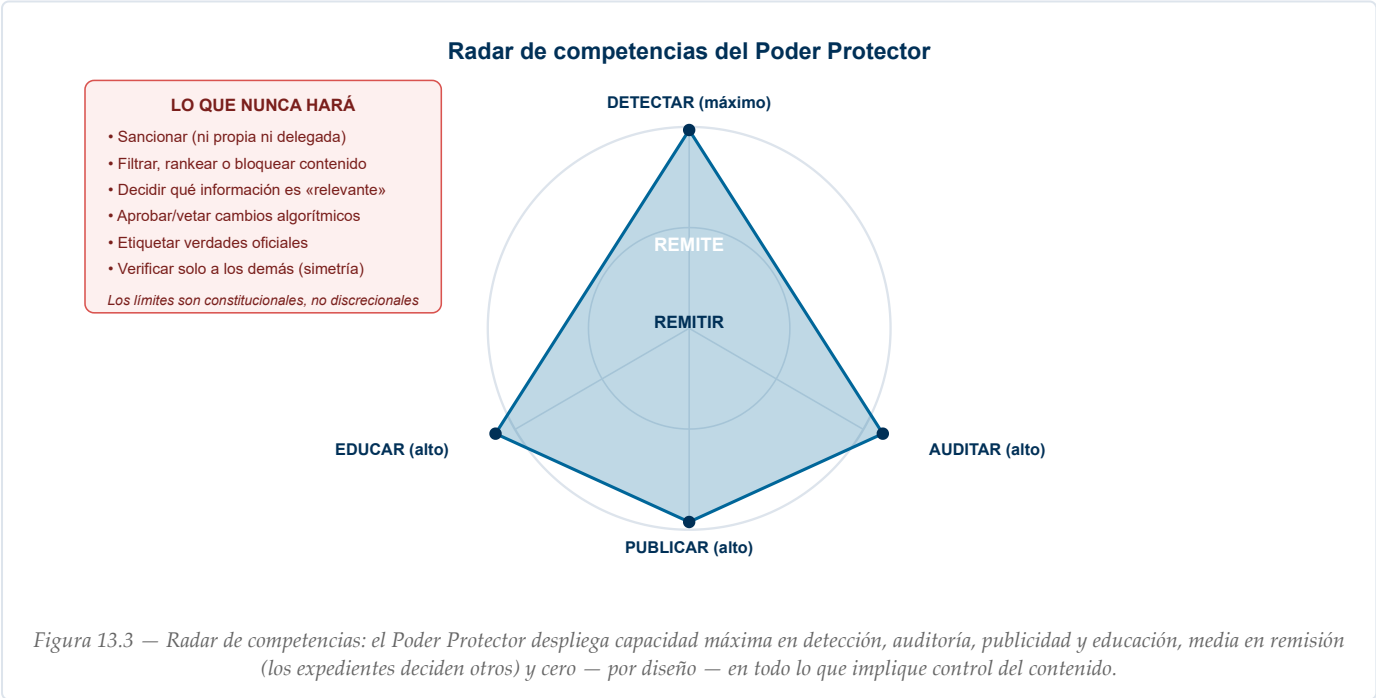
La lectura de la tabla es la tesis del capítulo: **Europa ya escribió la mayor parte del derecho que el Poder Protector haría cumplir.** El DSA ordena transparencia; el AI Act ordena vigilancia de sistemas; el Data Act ordena apertura; el Escudo defiende las elecciones. Lo que no existe es una institución pública con el mandato permanente, los recursos técnicos y la independencia constitucional para ejecutar todo eso de forma sistemática — mirar dentro de los sistemas, documentar, publicar y remitir, cada día, no solo cuando estalla un escándalo. Ese ejecutor ausente es exactamente el conjunto de competencias descrito en 13.2.

13.6 La matriz de transferencia de poder: 2026 → 2035+



13.7 Los límites constitucionales: qué puede y qué nunca hará

En un diseño donde la amenaza central es la manipulación, un poder público con herramientas forenses potentes necesita límites más nítidos que sus competencias. El diseño los eleva a rango de definición institucional — tan vinculantes como las cinco funciones:



Este radar es la respuesta institucional a la objeción clásica: «¿quién vigila al vigilante?». La respuesta del diseño es triple: **(1) límites constitucionales** — las prohibiciones de la figura 13.3 se inscriben en la propia definición del poder, reformable solo por el procedimiento del Capítulo 15; **(2) simetría** — el escáner y el Comprobador se aplican al propio PP; **(3) jurisdicción especializada** — cada acto del PP es recurrible ante la Cámara Especializada en Protección Digital y, en casación, ante el TJUE (Cap. 12). Un poder que no puede tocar el contenido, que se audita a sí mismo con las mismas herramientas y cuyos actos enjuician jueces independientes, tiene la respuesta incorporada.

13.8 Por qué estas competencias son urgentes

La urgencia no depende de escenarios especulativos. Depende de la convergencia verificada de tres tendencias:

1. **La ventana regulatoria se cierra en agosto de 2026.** El AI Act alcanza aplicabilidad plena el 2 de agosto de 2026; el Data Act ya es aplicable desde septiembre de 2025; el acto delegado del art. 40 DSA está adoptado. Si en los años de vigencia de ese acervo no existe un ejecutor sistemático, la experiencia de la política digital europea dice que el derecho se queda en el papel y las plataformas aprenden a cumplir el mínimo auditable.
2. **La manipulación se industrializa.** Los deepfakes y las operaciones FIMI documentadas por el EEAS son cada vez más baratos y eficaces; el tercer informe FIMI muestra campañas coordinadas contra procesos democráticos europeos que la detección actual encuentra después del daño electoral.
3. **La confianza informativa se erosiona estructuralmente.** El Reuters Institute lleva años documentando el descenso de la confianza y el desplazamiento hacia fuentes no editoriales (creadores, asistentes de IA) sin estándares de verificación. Cada ciclo electoral sin infraestructura de protección cognitiva amplifica la espiral: menos confianza, más manipulabilidad, menos participación.

El contrapeso institucional completado. El Ejecutivo, el Legislativo y el Judicial se equilibran entre sí — pero los tres operan en una esfera cognitiva cuya infraestructura la controlan actores privados y hostiles. Los tres poderes son hoy espectadores de la manipulación de la opinión que los legitima. El Poder Protector no es un cuarto rival de los tres: es el que asegura que los tres puedan seguir operando con una ciudadanía capaz de formarse juicios propios. No equilibra a los poderes: **protege el terreno sobre el que los tres se ejercen.**

13.9 Conclusión: recuperar el poder digital sin conquistarlo

1. **El poder digital existe y no está en manos democráticas.** No lo controla una conspiración: lo controla una infraestructura opaca de distribución, unos modelos de IA concentrados fuera de Europa y unos actores — domésticos y extranjeros — que aprenden a manipularla a bajo coste.
2. **El acervo para recuperar la vigilancia ya está escrito.** DSA, AI Act, Data Act, Escudo Europeo de la Democracia, Paquete de Soberanía: falta un ejecutor permanente, técnico e independiente. Ese es exactamente el hueco de las competencias del PP.
3. **Las competencias son cinco funciones protectoras con límites constitucionales.** Detectar, auditar, publicar, remitir, educar — y nunca sancionar, filtrar, priorizar ni etiquetar. El escáner forense cognitivo genera evidencia con doble verificación humana; los algoritmos de las plataformas siguen decidiendo la distribución, ahora a la vista.
4. **El Comprobador Ciudadano es una previsión prudente.** Verificación no vinculante de indicios, pseudonimizada, simétrica, en tres fases y sin presupuesto comprometido hasta que una evaluación independiente diga que vale la pena.
5. **La urgencia no admite espera.** La aplicabilidad plena del AI Act (agosto de 2026), la industrialización de la manipulación y la erosión estructural de la confianza convergen en los mismos años. Cada año sin ejecutor es un ciclo electoral desprotegido.

La tesis del capítulo en una frase: el Poder Protector no conquista el poder digital — lo ilumina. Y una esfera cognitiva iluminada, con sancionadores existentes al otro lado de los expedientes y jueces independientes detrás de cada acto, es más difícil de manipular y más difícil de censurar a la vez.

13.10 Fuentes y referencias verificadas

- **Eurobarómetro sobre la percepción de la desinformación (febrero de 2025):** un 36% de los europeos declara estar expuesto «a menudo» o «muy a menudo» a contenidos distorsionados o falsos.
- **Reuters Institute Digital News Report (edición 2026):** caída continuada de la confianza y del interés en noticias, auge de creadores individuales y del consumo informativo mediado por asistentes de IA.
- **Stanford AI Index (2026):** concentración de los modelos de IA punteros en EE. UU., liderazgo chino en publicaciones, avance europeo (Mistral) desde posición dependiente.
- **EDMO (Observatorio Europeo de los Medios Digitales):** estudios sobre actores de manipulación informativa, combinación de actores domésticos y extranjeros en Europa.

- **EEAS, tercer informe FIMI:** campañas de interferencia e manipulación informativa contra procesos democráticos europeos.
- **DSA (Reg. 2022/2065):** techos del 6%, auditorías, y acto delegado del art. 40 sobre acceso de investigadores a datos de plataformas adoptado el 2 de julio de 2025.
- **AI Act (Reg. 2024/1689):** techos del 7% de facturación mundial o 35M€, aplicabilidad plena el 2 de agosto de 2026.
- **Data Act (Reg. 2023/2854):** aplicable desde el 12 de septiembre de 2025.
- **Escudo Europeo de la Democracia (Comisión Europea, 12 de noviembre de 2025)** y Recomendación (UE) 2023/2829 sobre procesos electorales inclusivos y resilientes (2023).
- **Paquete de Soberanía Tecnológica y Cloud AI (Comisión Europea, 3 de junio de 2026):** Cloud and AI Development Act, Cloud Sovereignty Framework, reducción de dependencias, infraestructura europea.
- **Shoshana Zuboff (2019), *The Age of Surveillance Capitalism*** y trabajos del **Oxford Internet Institute:** marco analítico del poder de la infraestructura informacional.
- **Diseño institucional:** Capítulos 8 (doble verificación humano-IA), 12 (arquitectura, jurisdicción especializada, departamentos), 15 (base legal) y 16 (recursos propios).

Capítulo 14: Proceso de Transición

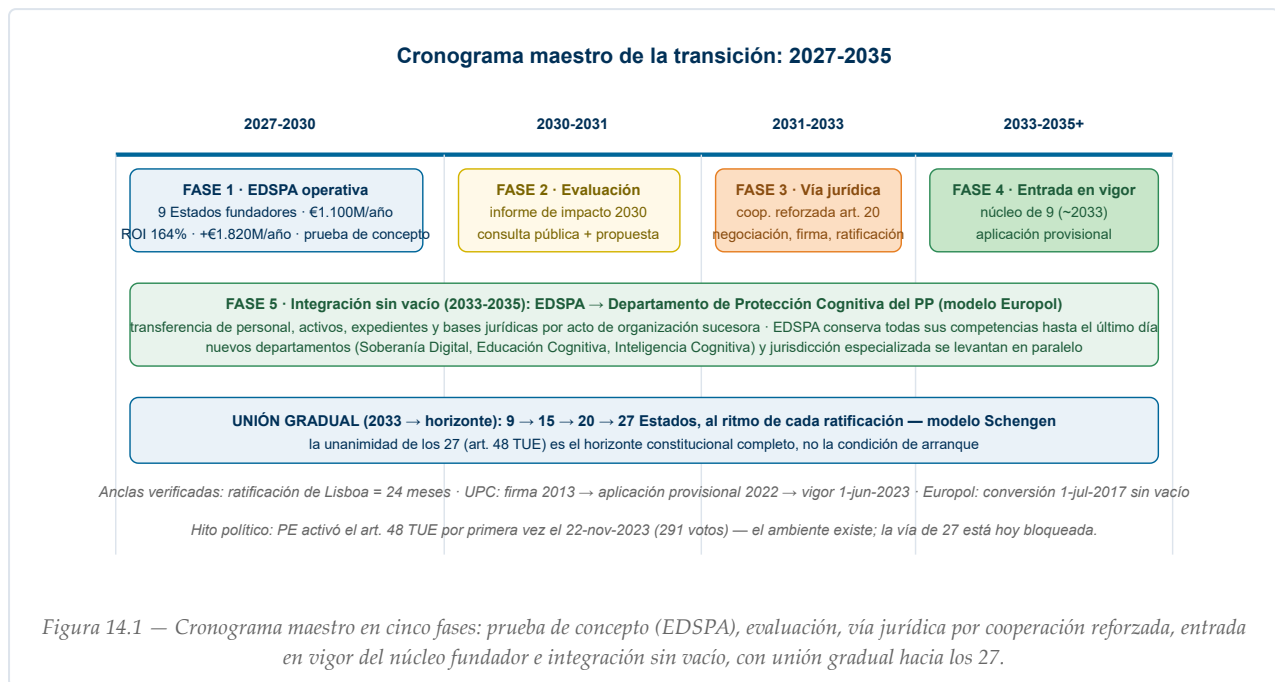
Resumen del capítulo

Este capítulo detalla el proceso paso a paso para transformar la EDSPA en el Poder Protector entre 2027 y 2035, sobre dos decisiones de fondo. Primera: **la vía constitucional realista** — una doble vía: **cooperación reforzada del art. 20 TUE con un núcleo fundador de 9 Estados** (el mismo legal, ya usado en el divorcio Roma III y la patente unitaria), con unión gradual al modelo Schengen y aplicación provisional (el precedente del Tribunal Unificado de Patentes, que empezó a funcionar así), y la **unanimidad de los 27 como horizonte**, no como condición de arranque. El precedente político es reciente y verificable: el 22 de noviembre de 2023 el Parlamento Europeo activó por primera vez en la historia el art. 48 TUE (291 votos a favor) y el Consejo Europeo no le dio curso — la vía de los 27 está hoy bloqueada, y el diseño asume esa realidad en vez de ignorarla. Segunda: **la transición respeta el protector puro**. La transferencia es de competencias protectoras, personal, activos y evidencia — la sanción sigue entera en la Comisión (DSA 6% / AI Act 7%). La financiación se remite al Cap. 16: recursos propios, sin multas ni impuestos como ingreso del PP — las multas que la Comisión imponga van a las arcas generales de la UE, no al presupuesto del poder que las motivó; y la exportación de la tecnología a otras democracias queda anotada como posible recurso propio futuro, nunca como supuesto del plan. La garantía central del proceso: **ni un día de vacío de protección**, con el precedente técnico de la conversión de Europol (2017) y del arranque del TUP (2023).

14.1 Los precedentes reales: Europa ya ha hecho esto tres veces

Precedente	Qué demuestra	Lección para la transición EDSPA → PP
Cooperación reforzada (art. 20 TUE)	Un mínimo de 9 Estados miembros puede avanzar en integración dentro de las estructuras de la UE sin esperar a todos: así nacieron el reglamento de divorcio Roma III (2010) y la patente unitaria	El núcleo fundador de 9 Estados del Capítulo 6 es legalmente suficiente: no hay que esperar a 27
Europol (Reg. 2016/794)	El 1 de julio de 2017 una organización intergubernamental de los Estados se convirtió en agencia de la UE «reemplazando y derogando» sus actos anteriores, con transferencia de personal y actividades sin un solo día de vacío	La integración de la EDSPA como Departamento de Protección Cognitiva puede hacerse por organización sucesora, heredando contratos, expedientes y bases jurídicas en un acto
Tribunal Unificado de Patentes	Acuerdo firmado en 2013; aplicación provisional desde 2022 (contratación de jueces y personal antes de la ratificación completa) y entrada en vigor el 1 de junio de 2023 con 17-18 Estados; Dinamarca lo ratificó tras referéndum (2014)	La aplicación provisional permite construir el PP de 2033 mientras se completa la ratificación, y el escalamiento gradual por grupo de Estados es viable y probado
Tratado de Lisboa	Firmado el 13 de diciembre de 2007, en vigor el 1 de diciembre de 2009: 24 meses de ratificación con un referéndum nacional rechazado y repetido (Irlanda 2008→2009) en el camino	Planificar 24 meses de ratificación es realista; un solo revés nacional no hunde el proceso si el diseño ya contempla la unión gradual
Parlamento Europeo, 22 de noviembre de 2023	Por primera vez en la historia, activó el procedimiento del art. 48 TUE pidiendo la convocatoria de una Convención (291 votos a favor, 274 en contra, 44 abstenciones); el Consejo Europeo no le dio curso	El ambiente constitucional existe pero la vía de la unanimidad está hoy bloqueada: el diseño de transición debe asumirlo, no fingir lo contrario
Conferencia sobre el Futuro de Europa (2022)	49 propuestas con más de 300 medidas, construidas con paneles de ciudadanos aleatorios, incluyendo reformas de Tratado	El método participativo ya está inventado y ensayado: la Convención del PP lo reutiliza con paneles ciudadanos sobre protección cognitiva

14.2 El cronograma maestro: cinco fases, 2027-2035



Fase 1: EDSPA operativa (2027-2030)

Los nueve Estados fundadores ponen la agencia en marcha con el presupuesto base de €1.100M/año. El objetivo no es solo proteger desde el primer día, sino **generar la evidencia que hace inevitable la reforma**: auditorías publicadas, expedientes remitidos, elecciones protegidas (incluidas las europeas de 2029), ROI del 164% y + €1.820M/año de beneficio neto documentados con la metodología del Capítulo 9. La EDSPA no pide fe: produce resultados auditables.

Fase 2: Evaluación y propuesta (2030-2031)

Informe de impacto trienal de la EDSPA con verificación externa; consulta pública paneuropea con paneles de ciudadanos aleatorios (método ya ensayado por la Conferencia sobre el Futuro de Europa); y propuesta formal de la Comisión Europea para una cooperación reforzada que institucionalice el Poder Protector. El argumento es el del Capítulo 11: la EDSPA funciona, pero es revocable por una mayoría política — la protección cognitiva necesita anclaje constitucional.

Fase 3: Vía jurídica (2031-2033)

Autorización del Consejo a la cooperación reforzada (mayoría cualificada, previo cumplimiento de los requisitos del art. 20 TUE), negociación del convenio constitutivo entre los Estados participantes, firma y **ratificación con 24 meses de margen** — el tiempo real que tardó Lisboa, con un revés nacional incluido. Para los Estados cuya constitución exige referéndum, el precedente danés del TUP (2014) muestra que estos procesos también se ganan en las urnas.

Fase 4: Entrada en vigor del núcleo (~2033)

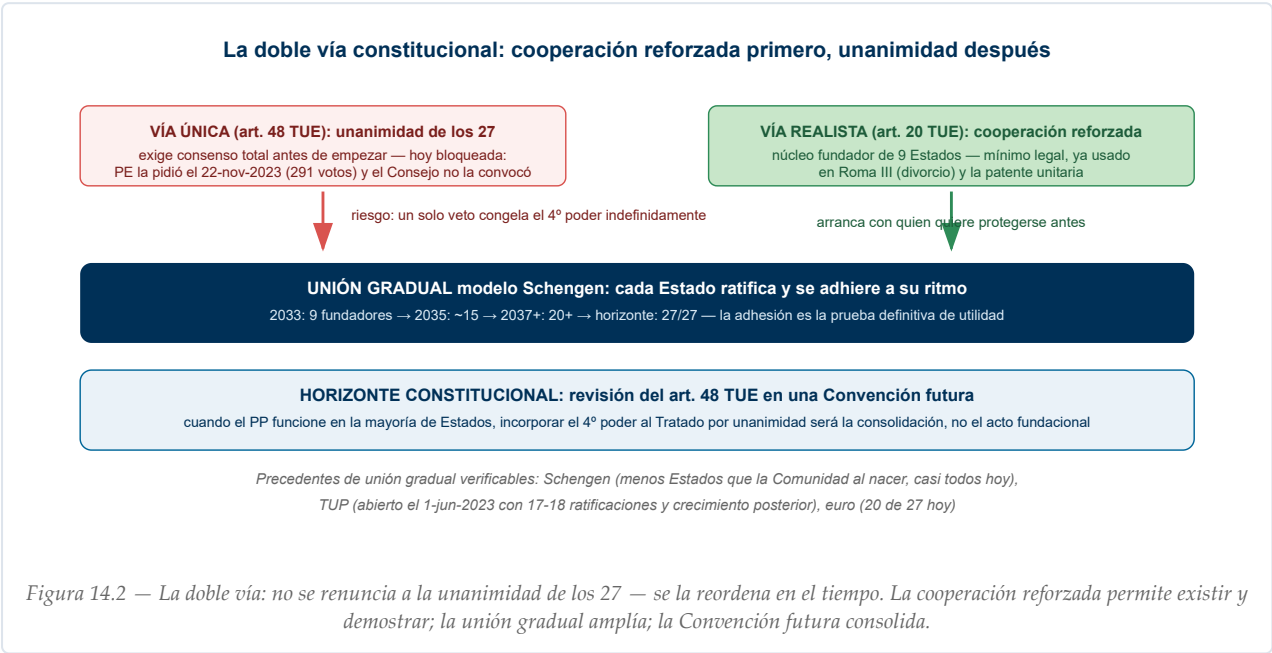
El Poder Protector nace con los Estados que ya han ratificado — no menos de 9 —, con **aplicación provisional** desde la firma para que los órganos (Consejo de Protección Cognitiva, dirección ejecutiva, inicio de la Cámara Especializada) estén contruidos y dotados el día uno, exactamente como el TUP contrató a sus jueces antes de abrir sus puertas.

Fase 5: Integración sin vacío (2033-2035) y unión gradual (2033 → horizonte)

Por un acto de organización sucesora al modelo del Reg. 2016/794 (Europol), la EDSPA se convierte en el Departamento de Protección Cognitiva del PP: personal, sede, sistemas, expedientes y bases jurídicas se transfieren en bloque, y la agencia conserva **todas** sus competencias hasta el último día. En paralelo se levantan los otros tres departamentos y la jurisdicción especializada del Capítulo 12. Los demás Estados se adhieren a su ritmo, cada

uno con su ratificación — el modelo Schengen: empezó con menos Estados que la Comunidad y hoy cubre la casi totalidad, incluidos países no miembros de la UE.

14.3 La doble vía constitucional: por qué nueve y no veintisiete

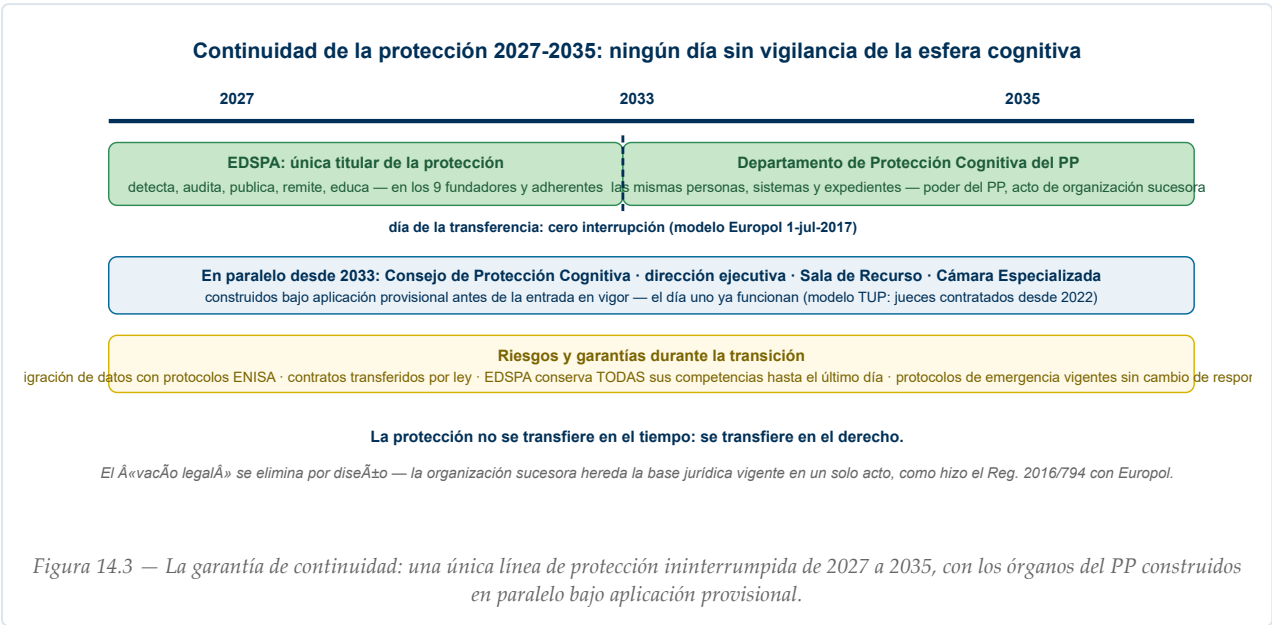


La razón de fondo no es táctica sino democrática: exigir unanimidad para *empezar* significa que el Estado más reacio — o más manipulado — decide si los demás pueden protegerse. La cooperación reforzada invierte esa lógica: quien quiere protección la tiene pronto, y quien espera no bloquea a nadie. Y la experiencia enseña que lo que funciona acaba atrayendo: Schengen, el euro y el TUP crecieron todos después de nacer pequeños.

14.4 Qué se transfiere — y qué no se toca

Elemento	EDSPA (2027-2033)	Poder Protector (2033-2035 en adelante)	Mecanismo
Competencias protectoras	Detectar, auditar, publicar, remitir, educar (Cap. 13)	Idénticas, con anclaje constitucional y cobertura de los Estados adheridos	Acto de organización sucesora (modelo Europol): bases jurídicas heredadas, no renegociadas
Sanción	Fuera de la agencia: Comisión (DSA 6% / AI Act 7%)	Sigue fuera: la transición no añade ni un poder sancionador	No se transfiere porque no existe en ninguno de los dos
Personal	1.500-2.000 empleados	Transferidos en bloque, contratos incluidos; ampliación gradual del Cap. 12	Transferencia automática de contratos (precedente Europol 2017)
Activos	Sede, sistemas forenses, escáner cognitivo, expedientes	Heredados íntegros el día uno	Inventario cerrado y auditado antes de la firma del convenio
Presupuesto	€1.100M/año (base)	Marco del Cap. 17: €2.600M base / €3.400M pleno, con recursos propios del Cap. 16	Migración por tramos conforme se incorporan departamentos y Estados
Ingresos por multas	Ninguno para la agencia	Ninguno para el PP: las multas que imponga la Comisión van a las arcas generales de la UE	Separación estructural para siempre el ojo que detecta de la mano que cobra

14.5 La garantía de continuidad: ni un día de vacío



14.6 Obstáculos y estrategias

Obstáculo	Riesgo	Estrategia	Ancla verificable
Estados que no se suman	Cobertura inicial parcial	No bloquear: cooperación reforzada desde 9, unión gradual, cada adhesión es publicidad del éxito	Art. 20 TUE (mínimo 9); Schengen y el euro crecieron tras nacer pequeños
Un revés en una ratificación	Retraso de meses o años	Margen de 24 meses en el cronograma; aplicación provisional mantiene el calendario de construcción	Lisboa tardó 24 meses con un referéndum repetido; TUP arrancó bajo aplicación provisional
Lobby de plataformas	Campañas contra la reforma, captura del debate	Transparencia total de las negociaciones; la propia EDSPA documenta y publica las operaciones de influencia que detecte	Registro de transparencia de la UE; DSA art. 40 (acceso a datos para investigadores)
Cambio de gobiernos	Retirada de apoyo político	Base transversal: los beneficios (ROI 164%, +€1.820M/año) y los expedientes son de todos los gobiernos; acuerdo firmado tras informes de impacto auditados	La adhesión a Schengen/euro sobrevivió a decenas de cambios de gobierno
Manipulación contra la reforma misma	Desinformación sobre «el ministerio de la verdad europeo»	El diseño mismo es la respuesta: límites constitucionales del Cap. 13 (jamás filtra, jamás sanciona, simetría anti-arma) y litigio público de cada mito con evidencia	Radar de límites del Cap. 13; simetría verificable del escáner
Fragilidad técnica de la migración	Pérdida de datos o capacidad	Protocolos de migración validados por ENISA, redundancia, inventario cerrado antes de la firma	Certificaciones y prácticas de las agencias descentralizadas de la UE

14.7 Indicadores de éxito de la transición

La transición se mide con **indicadores de proceso verificables** — cosas que realmente se pueden contar y auditar:

- **De protección:** auditorías algorítmicas completadas y publicadas por año; expedientes remitidos a la Comisión y resoluciones sancionadoras derivadas; elecciones europeas de 2029 y 2034 cubiertas sin incidentes graves de interferencia documentados sin respuesta.
- **De credibilidad económica:** ROI del 164% y beneficio neto de +€1.820M/año verificados externamente (metodología del Cap. 9B), presupuesto ejecutado con desviación inferior al 5%.

- **De ampliación:** Estados adheridos a la cooperación reforzada (9 → 15 → 20+); cobertura poblacional de la protección cognitiva; adhesiones tras cada ciclo electoral bien protegido.
- **De capacidad social:** avance de la alfabetización cognitiva hacia la meta de $\geq 90\%$ en 2038 (desde la línea de base real de la Década Digital: 80% objetivo 2030, ~55,6% verificado hoy).

14.8 Conclusión: una transición diseñada para no fallar

1. **El proceso no pide un milagro político: pide nueve gobiernos decididos.** El art. 20 TUE permite empezar con el núcleo fundador; Schengen, el euro y el TUP demuestran que las integraciones europeas exitosas nacen pequeñas y crecen por resultados.
2. **El cronograma está anclado en tiempos reales.** 24 meses de ratificación (Lisboa), aplicación provisional (TUP), organización sucesora sin vacío (Europol): cada fase copia un precedente que ya ocurrió, no una esperanza.
3. **La transición no diluye el protector puro: lo consolida.** No se transfieren poderes sancionadores porque no existen en ninguno de los dos niveles; las multas siguen en la Comisión y a las arcas de la UE; el PP llega a 2035 con más cobertura, más departamentos y el mismo arma de siempre: la luz.
4. **La vía de los 27 no se abandona: se reordena.** La unanimidad es el horizonte de consolidación en una Convención futura — cuando existir y funcionar sea el mejor argumento para el Tratado que aún no se puede aprobar hoy.

La tesis del capítulo en una frase: la EDSPA demuestra que la protección funciona; la cooperación reforzada permite que nueve Estados la hagan constitucional sin pedir permiso al más lento; y la unión gradual convierte cada año de resultados en el argumento que arrastra a los demás — hasta el día en que los 27 consoliden por unanimidad lo que la mayoría ya vive.

14.9 Fuentes y referencias verificadas

- **Art. 48 TUE** (procedimientos de revisión ordinario y simplificado) y **art. 20 TUE** (cooperación reforzada: mínimo 9 Estados): EUR-Lex, textos consolidados.
- **Resolución del Parlamento Europeo de 22 de noviembre de 2023** que activa por primera vez el art. 48 TUE y pide la convocatoria de una Convención (voto: 291 a favor, 274 en contra, 44 abstenciones; la resolución del 9-jun-2022 que pedía lo mismo se aprobó con 355:154:48).
- **Conferencia sobre el Futuro de Europa (2022):** informe final, 49 propuestas con más de 300 medidas, paneles de ciudadanos aleatorios; propuesta 39 sobre fin de la unanimidad y 38 sobre referéndums europeos.
- **Europol:** Reglamento (UE) 2016/794, que convirtió la organización intergubernamental en agencia de la UE el 1 de julio de 2017 «reemplazando y derogando» sus actos fundacionales, con transferencia de personal y actividades.
- **Tribunal Unificado de Patentes:** Acuerdo de 2013, aplicación provisional desde 2022, entrada en vigor el 1 de junio de 2023 con 17-18 Estados; referéndum danés de adhesión (25 mayo 2014, 62,5% a favor).
- **Tratado de Lisboa:** firma 13-dic-2007, entrada en vigor 1-dic-2009; ratificación completada con el depósito checo del 13-nov-2009; referéndum irlandés de 2008 (rechazo) y 2009 (aprobación).
- **Precedentes de cooperación reforzada:** Reglamento Roma III sobre divorcio (Reg. 1259/2010, 14→17 Estados participantes) y patente unitaria.
- **Schengen y el euro** como precedentes de unión gradual e integraciones de geometría variable.
- **Marcos propios del libro:** Cap. 9B (ROI 164%, +€1.820M/año), Cap. 6 (núcleo fundador de 9), Cap. 11 (EDSPA como paso necesario), Cap. 12 (arquitectura e integración 2033-2035), Cap. 13 (competencias del protector puro), Cap. 16 (recursos propios) y Cap. 17 (€2.600M/€3.400M).

Capítulo 15: Base Legal del Poder Protector

El derecho ya existe: valores, derechos fundamentales y jurisprudencia sostienen la protección cognitiva hoy — lo que falta no es base legal, es rango constitucional: y el poder que protege la democracia en la era digital se dota como un poder, no como un programa

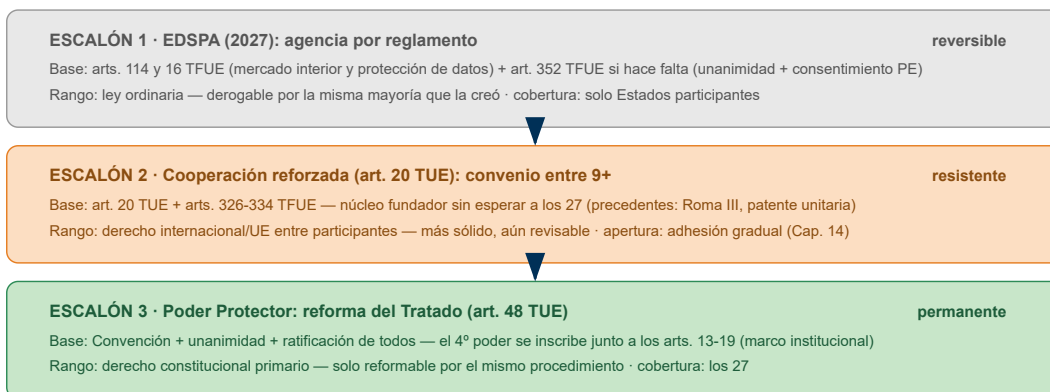
Resumen del capítulo

Este capítulo hace lo que anuncia su título: **demostrar que el derecho europeo ya sostiene la protección cognitiva — y que lo único que falta es rango**. La tesis es constructiva en tres niveles. Primero: el **principio de protección** ya está en el Tratado — el art. 2 TUE consagra la democracia entre los valores de la Unión, el art. 3 la defiende entre sus objetivos, y la Carta de Derechos Fundamentales protege la vida privada (art. 7), los datos personales (art. 8), la libertad de expresión e información (art. 11) y la tutela judicial efectiva (art. 47) — los cuatro derechos exactos que la manipulación digital vulnera. Segundo: la jurisprudencia del TJUE ya reconoció que la dignidad digital es justiciable — de *Digital Rights Ireland* a *Schrems II*. Tercero: el derecho positivo existente (DSA, AI Act, RGPD) ya ordena casi todo lo que el PP haría cumplir — pero lo ordena sin ejecutor permanente, y ninguna ley ordinaria puede crear un 4º poder: eso exige el art. 48 TUE (con la doble vía del Capítulo 14) o, en su caso, el art. 20 TUE. El capítulo añade una pieza propia: **la dotación de un poder**. Las democracias siguen ancladas en la era analógica — sus tres poderes se diseñaron cuando la opinión pública se formaba en la plaza, la prensa y la televisión, y ninguno vigila el terreno digital donde hoy se forman las voluntades. Meter a la democracia en la era digital exige un poder dimensionado como tal: de los 1.500-2.000 heredados de la EDSPA a **más de 15.000 efectivos en su madurez (2040+)** — todavía el más ligero de los cuatro poderes para la misión más nueva, financiado por el círculo recaudatorio virtuoso de sus propios expedientes (multas a las arcas de la UE, recursos propios del art. 311 TFUE) y por el contrapeso que ningún otro poder ofrece: el mayor empleador público europeo del juicio humano no automatizable frente a la IA. Y con una doctrina que fija el capítulo: un poder no se justifica por su viabilidad económica — se dota según su cometido; que además se pague solo (ROI 164%, Cap. 9B) es la cereza, no el pastel.

15.1 La jerarquía de bases jurídicas: tres escalones hacia el 4º poder

Nada del diseño del PP exige inventar derecho nuevo: exige **subir de escalón** en una jerarquía que ya existe. Cada escalón tiene su base, su rango y su reversibilidad — y el argumento del libro es que solo el tercero garantiza una protección que no dependa de una mayoría política anual.

Jerarquía de bases jurídicas: de la ley derogable al poder constitucional



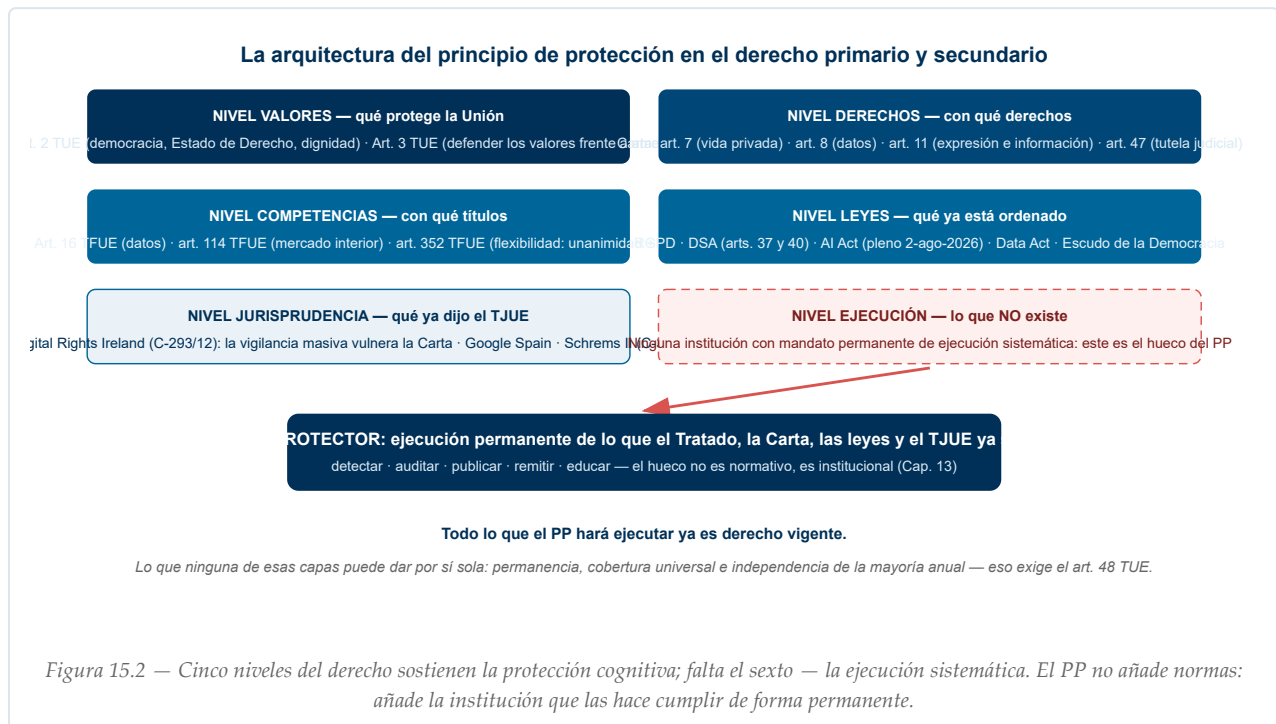
La protección cognitiva no cambia de contenido al subir de escalón: cambia de rango.

Y el rango es la garantía: lo que una mayoría no puede dar, otra mayoría no puede quitar.

Figura 15.1 — Los tres escalones de la base legal: la EDSPA puede fundarse mañana con derecho vigente; el 4º poder exige el art. 48 TUE — con la doble vía del Capítulo 14.

15.2 El principio de protección ya está en el Tratado

La objeción más común — «no hay base legal para un poder así» — confunde dos preguntas: si la UE *puede* proteger la esfera cognitiva, y si la UE *debe* hacerlo con rango constitucional. La primera ya está respondida por el derecho vigente:



La jurisprudencia que ya protege la esfera cognitiva

- **TJEU, *Digital Rights Ireland* (C-293/12 y C-294/12, 2014):** invalidó la Directiva de Retención de Datos porque la retención masiva e indiscriminada interfiere de modo especialmente grave con los derechos fundamentales — el tribunal ya dijo que la vigilancia total de la vida digital es incompatible con la Carta.
- **TJEU, *Google Spain* (C-131/12, 2014):** el derecho de supresión frente al buscador reconoce que el individuo controla su huella informativa: la autonomía informativa es un derecho operativo, no teórico.
- **TJEU, *Schrems II* (C-311/18, 2020):** el marco Privacy Shield cae porque la transferencia de datos a terceros países sin protección equivalente es ilícita — la soberanía de datos personales es exigible.
- La línea común: **la esfera cognitiva de la persona es jurídicamente protegible** — el TJUE la ha defendido caso a caso. El PP propone lo que la lógica de esa jurisprudencia ya apunta: protección sistemática, no solo reactiva.

La base financiera: el art. 311 TFUE

La autonomía financiera del Capítulo 16 tiene su fundamento en el **art. 311 TFUE**: la Unión se dota de recursos propios mediante una Decisión adoptada por unanimidad y aprobada por los Estados según sus normas constitucionales — el mismo mecanismo de la Decisión 2020/2053 que financió la recuperación pospandemia. Un poder constitucional estable necesita exactamente eso: ingresos que no renegocie cada presupuesto anual. La discusión de ingresos se remite al Cap. 16: **recursos propios sí, multas como ingreso propio jamás** — el círculo recaudatorio funciona por vía indirecta (véase 15.5).

15.3 Montesquieu y el 4º poder: la objeción y la respuesta

La objeción clásica

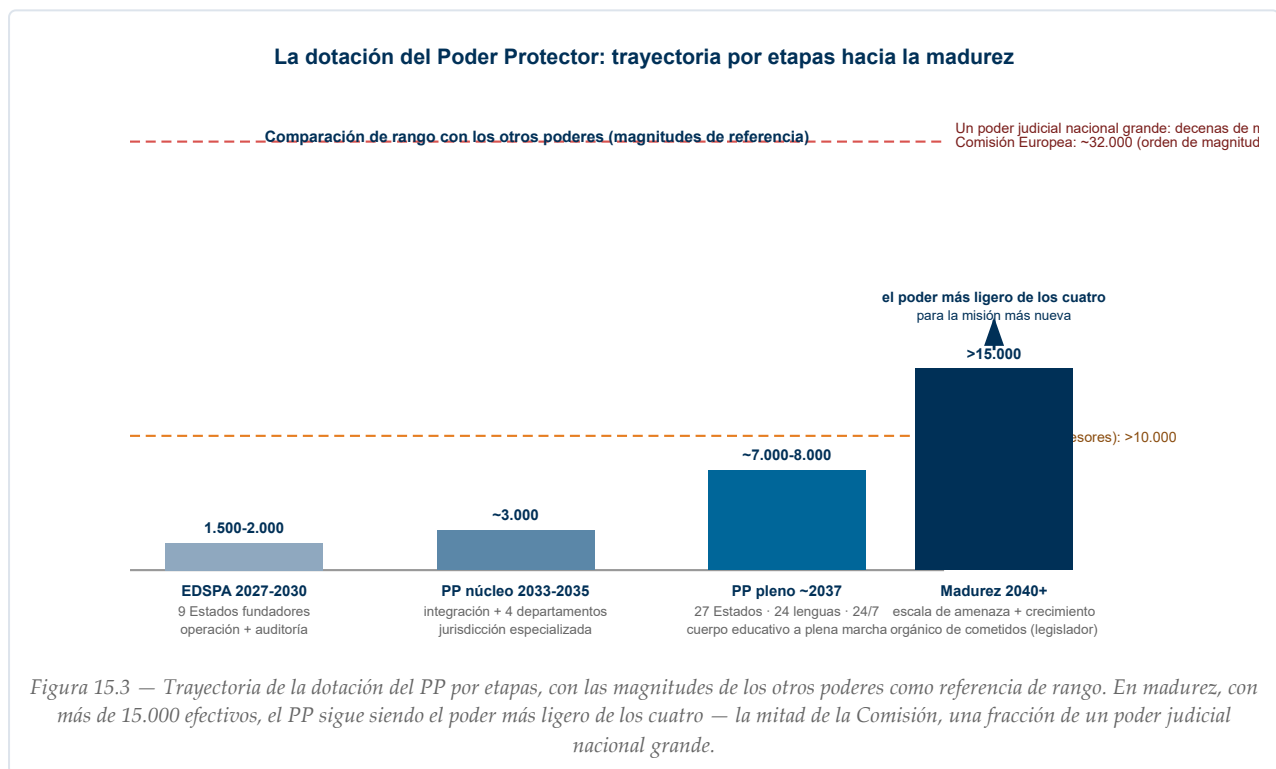
«La separación de poderes de Montesquieu (legislativo, ejecutivo, judicial) es la garantía de la libertad. Un 4º poder rompe el equilibrio.»

La respuesta tiene dos partes. La histórica: Montesquieu no enumeró una lista cerrada en *El Espíritu de las Leyes* (1748) — describió el principio de que **el poder debe frenar al poder**, y las constituciones han multiplicado los órganos que lo encarnan: tribunales constitucionales, bancos centrales independientes, defensores del pueblo, autoridades fiscales. Ninguno existía en 1748; todos son hoy ortodoxia democrática. La funcional: los tres poderes clásicos operan hoy en una esfera cognitiva que no controlan — y un poder que no controla el terreno de la opinión pública que lo legitima no equilibra nada: **está ciego**. El PP no añade un competidor a los tres: asegura que los tres puedan ver. Y a diferencia de un 4º poder sancionador — que sería un peligro real — este está diseñado sin la herramienta que haría temible a cualquier poder: **no puede castigar, solo iluminar** (Cap. 13). La separación de poderes no se rompe con un poder que publica: se rompería con un poder que calla, filtra y castiga a la vez.

15.4 La dotación de un poder: meter a la democracia en la era digital

Las democracias europeas siguen ancladas en la era analógica. Sus tres poderes se diseñaron — y se dotaron — cuando la opinión pública se formaba en la plaza, la prensa y la televisión: el legislativo para deliberar en cámara, el ejecutivo para administrar territorios, el judicial para enjuiciar casos. Hoy las voluntades se forman en sistemas de recomendación opacos, operados mayoritariamente desde otra jurisdicción, y ninguno de los tres poderes vigila ese terreno. **Ese es el anacronismo constitucional del siglo XXI**, y corregirlo no es crear «una agencia más»: es dotar a la democracia del poder que le falta para existir en la era digital. Y un poder se dota como se dotan los poderes.

La presencia física sigue tres categorías: proximidad, coordinación, excelencia — con el criterio de mérito y convocatoria abierta, y una **trayectoria por etapas** en la que cada salto tiene un disparador contable: adhesiones de Estados, cobertura de la misión, volumen de amenaza y las ampliaciones de cometidos que el legislador autorice con el tiempo como le ha ocurrido a todos los poderes europeos.



Por qué la cifra es la de un poder, no la de una agencia

Tres masas de personal hacen inevitable la trayectoria, y ninguna es burocracia:

- **La escala real de la operación.** Vigilancia forense continua de la esfera cognitiva de ~450 millones de personas en 27 Estados y 24 lenguas oficiales es una operación de turnos y cobertura continua: operadores del escáner forense, verificadores humanos (la doble verificación del Cap. 8 es deliberadamente no automatizable — es el corazón del diseño), auditores de plataformas por región y lengua, oficinas nacionales que a madurez operan con 100-150 personas. Este bloque solo ya supera el techo de la vieja proyección de «agencia».
- **El cuerpo de educación cognitiva.** La meta de alfabetización $\geq 90\%$ en 2038 es un programa del tamaño de un sistema educativo: formadores, diseñadores instruccionales, entrenadores, coordinación con los sistemas

escolares de 27 países. La educación no se escala solo con software — se escala con docentes.

- **El crecimiento orgánico de todo poder.** Todos los poderes europeos han crecido en cometidos y personal con el tiempo — la Comisión de unos pocos miles a ~32.000; Frontex de decenas de analistas a un cuerpo estatutario de 10.000 fijado para 2027. El PP no será la excepción: entre 2033 y 2040 el legislador autorizará ampliaciones — el Comprobador Ciudadano del Cap. 13 es solo la primera prevista, y sus necesidades de personal ya están dentro del horizonte de madurez, sin cifrarse aparte. Lo que no crece es la *naturaleza* de sus poderes: los límites constitucionales del Cap. 13 congelan qué puede hacer; las etapas solo escalan cuánto de lo mismo.

El contrapeso de la era IA: el mayor empleador público del juicio humano no automatizable

La IA elimina en la economía el juicio humano *rutinario* — redacción estándar, análisis básico, atención, diseño simple. El PP crea en Europa el mayor conjunto de empleos públicos de juicio humano *no rutinario*: verificar evidencia forense, supervisar auditorías, educar cognitivamente, ejercer criterio ante la ambigüedad. Y el diseño lo garantiza: la doble verificación humano-IA del Cap. 8 no es una fase transitoria hacia la automatización completa — es un principio institucional. Cada mejora de la IA del escáner no reduce el personal: **aumenta el volumen de hallazgos que exigen verificación y juicio humanos**. Mientras el resto de la economía descubre cuántos empleos puede prescindir del criterio de las personas, el PP es la institución europea que más criterio humano contrata — y lo hará cada año más. Frente al tsunami de destrucción de empleo cognitivo rutinario, Europa tendría un polo de reabsorción especializada: operadores, controladores, diseñadores, entrenadores, formadores — prevención, educación, supervisión.

15.5 El financiamiento de un poder: el círculo recaudatorio virtuoso

¿Y quién paga a un poder de más de 15.000 efectivos? La pregunta tiene dos respuestas — una contable y una doctrinal — y las dos juegan a favor del diseño.

La contable: el círculo recaudatorio. Cada expediente forense que el PP remite y la Comisión convierte en sanción (DSA hasta 6%, AI Act hasta 7%) ingresa en **las arcas generales de la UE** — y de esas arcas, vía los recursos propios del art. 311 TFUE, se dota el presupuesto del PP. El círculo es virtuoso y estructuralmente separado, como exige el protector puro: **el poder que detecta nunca cobra lo que detecta** — pero la Unión que lo dota sí ingresa lo que su trabajo produce. Y la magnitud ya no es teoría: la Comisión ha impuesto bajo el acervo digital multas de miles de millones de euros (Google Shopping, Android, Apple...), y cada una agravó la disciplina del mercado europeo. Un PP sistemático multiplicaría ese flujo: no como ingreso propio del poder (jamás), sino como flujo que hace que la Unión entera gane con cada expediente. La actividad del PP, que cuesta, es la misma actividad que recauda.

La doctrinal: un poder no necesita ser viable — necesita cumplir su cometido. A nadie se le ocurre preguntar si el poder judicial «es rentable», o si el parlamento «se paga solo»: se les dota lo que su función constitucional exige, porque sin ellos no hay democracia que pueda permitirse el lujo de calcularlo. El PP pertenece a esa categoría: es la condición para que las democracias existan en la era digital, y por eso se dota según su cometido, no según su rentabilidad. Que además — como demostró el Capítulo 9B con metodología verificable — arroje un ROI del 164% y un beneficio neto de +€1.820M/año, lo convierte en un caso casi único en la historia constitucional: **un poder que se justifica sin la economía y que, sin embargo, la economía lo respalda**. La viabilidad es la cereza sobre el pastel; el pastel es la democracia protegida.

Dimensión	Cifra	Fundamento
Presupuesto	€2.600M/año base / €3.400M pleno (Cap. 17)	En contexto real: el presupuesto UE 2026 es de €192.800M en compromisos; la Sección del Consejo Europeo + Consejo es de €739,6M — el PP pleno es una institución de presupuesto de gran órgano de la UE, coherente con su rango
Financiación	Recursos propios (Cap. 16, art. 311 TFUE)	Mecanismo probado (Decisión 2020/2053); sin multas ni impuestos como ingreso propio del PP — el círculo recaudatorio funciona por vía indirecta: las multas de la Comisión sobre expedientes del PP nutren las arcas de la UE que lo dota
Empleo directo	1.500-2.000 (EDSPA) → ~3.000 (núcleo) → ~7.000-8.000 (pleno ~2037) → >15.000 (madurez 2040+)	Trayectoria por etapas con disparadores contables (Fig. 15.3); el contrapeso del juicio humano no automatizable frente a la IA
Retorno	ROI 164% a 5 años; +€1.820M/año de beneficio neto	Cap. 9B — argumento adicional, no justificación: el poder se dota según su cometido
Talento	Polo europeo de especialización en protección cognitiva	Estabilidad del rango constitucional + centros de excelencia por convocatoria (modelo ERC): la carrera europea de la tecnología cívica

15.6 Conclusión: la base legal existe; lo que falta es rango — y dotación de poder

- La UE ya tiene el mandato de proteger la esfera cognitiva.** Valores (art. 2 TUE), objetivos (art. 3 TUE), derechos (Carta, arts. 7, 8, 11, 47), competencias (arts. 16 y 114 TFUE, art. 352 si hiciera falta) y jurisprudencia (Digital Rights Ireland, Google Spain, Schrems II): la protección cognitiva es la ejecución pendiente de derecho vigente.
- Lo que falta no es base: es rango y ejecutor.** Para eso están el art. 48 TUE (vía completa) y el art. 20 TUE (vía fundadora) — la doble vía del Capítulo 14.
- La objeción de Montesquieu se responde con el diseño.** El principio es que el poder frene al poder; el PP añade el contrapeso que falta y llega sin la herramienta del peligro: no sanciona, no filtra, solo ilumina, con jurisdicción independiente detrás de cada acto.
- Y se dota como lo que es: un poder.** Las democracias ancladas en la era analógica necesitan el poder que las introduzca en la era digital — con una trayectoria de dotación que va de los 1.500-2.000 heredados de la EDSPA a más de 15.000 efectivos en su madurez 2040+, financiado por el círculo recaudatorio de sus propios expedientes y por recursos propios, y convertido en el mayor polo europeo de empleo del juicio humano no automatizable frente a la IA. Un poder no necesita ser viable: necesita hacer bien su cometido — y este, además de cumplirlo, se paga solo.

La tesis del capítulo en una frase: el derecho europeo lleva una década ordenando y defendiendo la protección cognitiva; lo que necesita es darle rango de Tratado y dotación de poder — porque una democracia del siglo XXI no se protege con una agencia del siglo XX, sino con el cuarto poder que la trae a la era en la que sus ciudadanos ya viven.

15.7 Fuentes y referencias verificadas

- Tratados (EUR-Lex, textos consolidados):** art. 2 TUE (valores), art. 3 TUE (objetivos), arts. 20 y 48 TUE (cooperación reforzada y revisión), arts. 13-19 TUE (marco institucional), art. 16 TFUE (protección de datos), art. 114 TFUE (mercado interior), art. 352 TFUE (cláusula de flexibilidad: unanimidad + consentimiento del PE), art. 311 TFUE (recursos propios), arts. 326-334 TFUE (cooperación reforzada).
- Carta de Derechos Fundamentales:** arts. 1 (dignidad), 7 (vida privada), 8 (protección de datos), 11 (libertad de expresión e información) y 47 (tutela judicial efectiva).
- Jurisprudencia del TJUE:** Digital Rights Ireland, asuntos acumulados C-293/12 y C-294/12 (8-abr-2014); Google Spain, C-131/12 (13-may-2014); Schrems II, C-311/18 (16-jul-2020).
- Presupuestos verificados:** presupuesto UE 2026: €192.800M en compromisos / €190.100M en pagos (firmado 26-nov-2025); Sección II Consejo Europeo + Consejo: €739,6M en 2026.

- **Magnitudes institucionales (órdenes de magnitud, no cifras presupuestarias):** Comisión Europea ~32.000 funcionarios y agentes; personal del PE (institucional + grupos políticos) superior a 10.000; los poderes judiciales nacionales de los Estados grandes emplean decenas de miles de personas.
- **Precedente de crecimiento orgánico:** Frontex, de decenas de analistas en 2004 a un cuerpo estatutario de 10.000 fijado para 2027 por el legislador; ampliaciones sucesivas de plantilla también en Europol y en la duplicación de jueces del Tribunal General.
- **Recursos propios:** Decisión (UE, Euratom) 2020/2053 sobre el sistema de recursos propios (art. 311 TFUE).
- **Derecho positivo ejecutable:** RGPD (2016/679), DSA (2022/2065, art. 40 y acto delegado jul-2025), AI Act (2024/1689, pleno 2-ago-2026), Data Act (2023/2854).
- **Doctrina:** Montesquieu, *Del espíritu de las leyes* (1748) — el principio del poder que frena al poder; su desarrollo institucional posterior.
- **Marcos propios del libro:** Cap. 8 (doble verificación humano-IA), Cap. 9B (ROI 164%, +€1.820M/año), Cap. 12 (arquitectura, 1.500-2.000 empleados EDSA), Cap. 13 (protector puro, Comprobador), Cap. 14 (doble vía), Cap. 16 (recursos propios), Cap. 17 (€2.600M/€3.400M; 55.000-68.000 empleos del ecosistema).

Capítulo 16: El Financiamiento de un Poder — Recursos Propios

Un poder no pide presupuesto cada enero: el art. 311 TFUE dota a la Unión de ingresos que ninguna mayoría anual puede retacear — y el Poder Protector se financia con el mecanismo que ya existe, no con multas ni impuestos propios

Resumen del capítulo

Financiar un poder no es presentar un plan de negocio: **el poder que detecta nunca cobra lo que detecta**. Este capítulo se centra en lo que su título promete: **la autonomía financiera como condición de la independencia institucional**. La tesis es constructiva en tres niveles. Primero: el mecanismo ya existe — el **art. 311 TFUE** permite dotar a la Unión de recursos propios mediante una Decisión adoptada por unanimidad y ratificada por los 27 Estados según sus normas constitucionales: exactamente lo que hizo la Decisión 2020/2053 (2020) que financió la recuperación pospandemia y creó el recurso plástico. Segundo: el momento es el mejor posible — la Comisión propuso el 16-jul-2025, dentro del MFF 2028-2034, el mayor rediseño de los ingresos de la UE en una generación (CBAM, ETS, residuos electrónicos, tasa e-commerce, ETIAS; ~€410.000M adicionales estimados 2028-2035): **la Unión ya está rediseñando cómo se paga a sí misma, y el recurso propio del PP llega a una mesa que ya está puesta**. Tercero: la escala es la de una institución, no la de un programa — el PP pleno (€3.400M/año) equivale a **≈1,8% de los ingresos de la UE de 2026 (€190.091M)**, menos del 0,02% del RNB de la Unión, y el círculo recaudatorio del Cap. 15 no es teoría: las multas del acervo digital ya impuestas por la Comisión (más de €11.000M solo del caso Google, más las primeras del DMA: Apple €500M, Meta €200M) ingresan hoy en las arcas de la UE como «otros ingresos» del presupuesto. El capítulo cierra con el horizonte acordado: la exportación de tecnología de protección cognitiva a democracias como **posible recurso propio futuro — no como supuesto del plan** — y con la doctrina del Cap. 15: un poder no necesita ser viable; necesita cumplir su cometido. Que además arroje un ROI del 164% y +€1.820M/año (Cap. 9B) es la cereza, no el pastel.

16.1 El principio constitucional: un poder no pide presupuesto cada enero

Toda institución de la UE se financia con cargo al presupuesto general — pero un **poder constitucional** necesita algo más: que su dotación no dependa del humor de la negociación anual. La diferencia entre una agencia y un poder no está en lo que hacen: está en lo que *nadie puede quitarles*. El presupuesto de una agencia se renegocia cada ejercicio en el procedimiento del art. 314 TFUE; el Treaty rank de un poder se dota en el derecho primario.

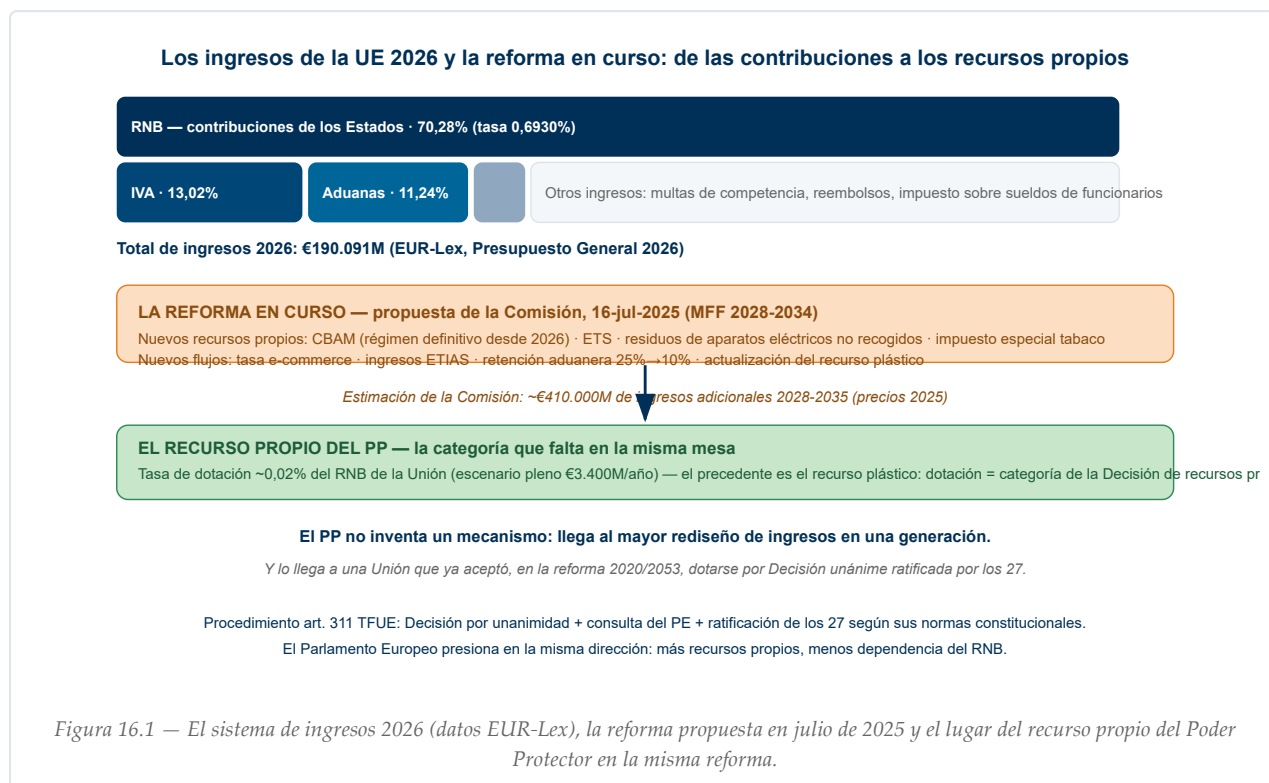
El Tratado ya resolvió este problema para la Unión entera. El **art. 311 TFUE** dispone que la Unión se dota de **recursos propios** para financiar su presupuesto, mediante una Decisión del Consejo adoptada por **unanimidad**, previa consulta del Parlamento Europeo, y aprobada por los Estados miembros «**de conformidad con sus respectivas normas constitucionales**» — es decir, con el mismo nivel de ratificación que una reforma de Tratado. No es un procedimiento inventado para el PP: es el que ha dotado cada gran salto institucional europeo, y el más reciente en el tiempo: la **Decisión (UE, Euratom) 2020/2053** (14-dic-2020), ratificada por los 27 y en vigor desde el 1-jun-2021, que financió la recuperación pospandemia y creó el primer recurso propio nuevo en décadas: la contribución basada en **residuos de envases plásticos no reciclados**.

Por qué el plástico importa aquí: cuando la Unión quiso financiar algo nuevo y prioritario (la reconstrucción pospandemia), no recurrió a multas ni a impuestos ad hoc: inscribió una categoría de dotación en la Decisión de recursos propios y la ratificaron los 27. **Ese es exactamente el diseño del PP:** su dotación entra en la Decisión de recursos propios como categoría propia (una tasa de dotación de ~0,02% sobre el RNB de la Unión en el escenario pleno), con la garantía de que ninguna mayoría anual puede retacear lo que el Tratado ordena dotar.

16.2 El sistema actual y su reforma: la ventana 2025-2026

El sistema de recursos propios vigente descansa sobre cuatro patas — y una de ellas soporta casi todo el peso. Los ingresos presupuestarios de 2026 (€190.091M) se financian así: **contribuciones basadas en el RNB, 70,28%** (tasa uniforme 0,6930%); **recursos IVA, 13,02%** (tasa 0,30% sobre bases topeadas al 50% del RNB); **recursos propios**

tradicionales (derechos de aduana; los Estados retienen el 25% en concepto de costes de recaudación), **11,24%**; y el **recurso plástico**, **3,59%**. En suma: casi tres cuartas partes del presupuesto dependen de cheques que firman los Estados cada año según su RNB — el «juste return» que la doctrina presupuestaria lleva décadas señalando como la debilidad estructural del sistema.

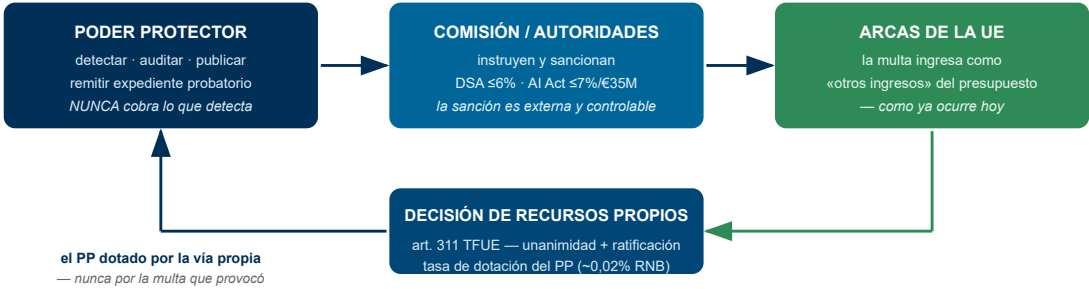


Por eso la ventana temporal importa. La reforma de los recursos propios ya está sobre la mesa con paquete completo (Decisión de recursos propios y MFF 2028-2034, con segundo paquete sectorial el 3-sep-2025), y el procedimiento — unanimidad y ratificación — es **el mismo que exigirá el Tratado del PP (art. 48 TUE)**. Las dos reformas pueden viajar juntas: cuando la Convención redacte el Tratado del 4º poder, la Decisión de recursos propios de su dotación puede tramitarse en paralelo, con la misma coalición fundadora que ratifique ambos. **Un solo acto político dota al poder y lo financia.**

16.3 La regla del protector puro: lo que el PP nunca cobra

La financiación del PP es la contrapartida exacta de su diseño de protector puro (Cap. 13): **cinco verbos — detectar, auditar, publicar, remitir, educar — y ninguno es cobrar**. Las multas que sus expedientes provocan las impone siempre la Comisión (DSA hasta 6% de la facturación mundial; AI Act hasta 7% o €35M) o las autoridades nacionales; y el dinero entra en **las arcas generales de la UE**, donde ya entran hoy: las multas de competencia y las del acervo digital son «otros ingresos» del presupuesto general.

El círculo recaudatorio: el PP detecta, la Unión cobra — separados por diseño



Ya verificado con dinero real: Google Shopping €2.420M · Android €4.340M · AdSense €1.490M · adtech €2.950M · DMA: Apple €500M + Meta €200M
Más de €11.000M ingresados o ordenados en el acervo digital — parte bajo recursos judiciales — equivalen a más de 3 años del PP pleno.

Figura 16.2 — El círculo recaudatorio virtuoso del Cap. 15, con la prueba de que ya funciona: las multas del acervo digital ya entran en el presupuesto de la UE como «otros ingresos».

La magnitud deja de ser especulación en el momento en que se cuentan los expedientes que ya existen. La Comisión ha impuesto sobre una sola empresa, en una sola década, más de **€11.000M** en el ámbito digital (Google Shopping €2.420M en 2017, confirmado por el Tribunal General en 2021; Android €4.340M en 2018; AdSense €1.490M en 2019; adtech €2.950M en septiembre de 2025), y estrenó el acervo de mercados digitales con las primeras multas DMA (23-abr-2025): **Apple €500M y Meta €200M**. Todo ese dinero ingresó en el presupuesto general de la UE. La diferencia entre hoy y el PP no es el mecanismo — es la *sistematicidad*: lo que hoy depende de investigaciones episódicas y laboriosas pasaría a ser el flujo constante de un poder que audita en permanencia. La Unión entera, no el PP, es la beneficiaria de ese flujo.

16.4 El recurso propio del Poder Protector: escala y diseño

¿Y cuánto cuesta dotar así a un poder? La escala exacta, con los ingresos verificados de 2026 (€190.091M):

Dimensión	Cifra	Fundamento y contexto verificado
Dotación anual	€2.600M base / €3.400M pleno (Cap. 17)	El marco del Cap. 17, sin cambios; la dotación crece con la trayectoria de personal del Cap. 15 (1.500-2.000 → >15.000 en madurez 2040+)
Peso en el presupuesto de la UE	≈1,8% de los ingresos de 2026 (€3.400M/€190.091M); ~1,4% en el escenario base	Ancla de escala: el PP pleno es una institución de ~2 euros de cada 100 del presupuesto de la Unión — el presupuesto de un gran órgano, no el de un programa
Peso en la economía de la UE	Menos del 0,02% del RNB de la Unión (orden de magnitud)	Una tasa de dotación del art. 311 TFUE comparable en diseño al recurso plástico (€0,80/kg): una línea en la Decisión, no un impuesto nuevo a terceros
Procedimiento	Decisión de recursos propios: unanimidad + consulta PE + ratificación de los 27	Art. 311 TFUE; mismo procedimiento que la Decisión 2020/2053 — y el mismo calendario posible que el Tratado del PP (art. 48 TUE): una sola coalición fundadora ratifica ambos
Retorno (argumento adicional)	ROI 164% a 5 años; + €1.820M/año de beneficio neto	Cap. 9B, metodología verificable — pero la dotación se justifica por el cometido, no por la rentabilidad (Cap. 15): un poder no necesita ser viable, necesita cumplir su cometido

La lección de los fracasos: por qué el recurso del PP es distinto

La historia de las finanzas europeas está llena de recursos propuestos y nunca nacidos. El **impuesto sobre transacciones financieras** se tramita en cooperación reforzada desde 2013 — y sigue estancado más de una década después. El **gravamen digital europeo** se aparcó en 2021 a la espera del acuerdo fiscal global de la OCDE (Pillar 1), del que EE.UU. se retiró en enero de 2025; los DST siguen siendo impuestos nacionales y la vía europea es hoy un debate. La lección es doble. Primero: **los recursos que fracasan son impuestos a terceros** — recaudados sobre alguien que se opone con todos sus recursos. Segundo: **el único recurso propio nuevo que ha nacido (el plástico, 2020/2053) no es un impuesto a terceros: es una asignación de dotación** — y ese es exactamente el diseño del PP. Su recurso no grava a nadie: asigna, por unanimidad y ratificación, la porción de recursos propios que el Tratado ordena dedicar a la protección de la esfera cognitiva. Ninguna empresa puede vetarlo; solo los 27 — y los 27 son quienes ratifican el Tratado.

16.5 El horizonte: exportación como posible recurso futuro, no supuesto

El capítulo cierra con el horizonte acordado en el Cap. 14: la exportación de tecnología de protección cognitiva a democracias es **un posible recurso propio futuro de la Unión — no un supuesto del plan**. El razonamiento es de dirección, no de cifra: el PP crea competencias (forense, auditoría algorítmica, educación cognitiva) que otras democracias querrán adquirir conforme la manipulación transfronteriza las alcance; si esa demanda se materializa, sus frutos deben entrar en el mismo círculo que las multas — **en las arcas de la UE, nunca en la caja del PP** — y podrán, algún día, inscribirse en la Decisión de recursos propios como categoría nueva. El capítulo no proyecta ingresos por ello: registra la puerta y quién tiene la llave (los 27 por unanimidad). El valor geopolítico de exportar un *modelo* — protección democrática frente a control autoritario — no necesita cifras inventadas para ser real, y el ecosistema que lo haría posible (55.000-68.000 empleos, Cap. 17) ya está cuantificado en su capítulo propio.

16.6 Conclusión: financiar un poder como se financian los poderes

1. **El mecanismo existe y está en uso.** Art. 311 TFUE, Decisión 2020/2053, recurso plástico: la Unión ya sabe dotarse por unanimidad y ratificación de los 27 — el PP usa el procedimiento que ya funciona, no uno inventado.
2. **El momento es una ventana.** La propuesta de reforma del 16-jul-2025 (MFF 2028-2034 y nuevos recursos propios: CBAM, ETS, e-commerce, ETIAS; ~€410.000M estimados 2028-2035) pone la mesa en la que el recurso del PP cabe — y el Parlamento Europeo empuja en la misma dirección. El Tratado del PP y su dotación pueden ratificarse juntos, con la misma coalición fundadora.
3. **La regla del protector puro es financiera también.** El PP no cobra multas ni impuestos: detecta, y la Unión cobra — y las multas ya entran hoy en las arcas de la UE (más de €11.000M en el caso Google; las primeras del DMA en 2025). El círculo recaudatorio beneficia a la Unión entera, nunca al poder que detecta.
4. **La escala es la de una institución.** ≈1,8% de los ingresos de la UE de 2026 en el escenario pleno, menos del 0,02% del RNB: una tasa de dotación en la Decisión de recursos propios, comparable en diseño al recurso plástico — dotada según el cometido (Cap. 15), y respaldada además por el ROI del 164% del Cap. 9B.
5. **Y el horizonte queda registrado, no presumido.** La exportación a democracias: posible recurso propio futuro en la misma vía — las arcas de la UE y la unanimidad de los 27 — sin cifras mágicas que nadie puede verificar.

La tesis del capítulo en una frase: un poder que depende del presupuesto anual no es un poder — es una agencia esperando su recorte; el Poder Protector se financia como se financia la Unión misma: con recursos propios del art. 311 TFUE, dotados por unanimidad y ratificados por los 27, para que la protección de la esfera cognitiva no dependa nunca del humor de una mayoría de enero.

16.7 Fuentes y referencias verificadas

- **Derecho primario:** art. 310 TFUE (unidad, universalidad, equilibrio y especificación del presupuesto), art. 311 TFUE (recursos propios: unanimidad + consulta del PE + aprobación según normas constitucionales), art. 314 TFUE (procedimiento presupuestario anual), art. 325 TFUE (lucha antifraude), art. 48 TUE (revisión de los Tratados).

- **Decisión de recursos propios:** Decisión (UE, Euratom) 2020/2053, de 14-dic-2020 (recurso plástico, correcciones GNI para varios Estados, ratificada por los 27; en vigor 1-jun-2021, aplicada desde 1-ene-2021); Reglamento (UE) 2021/770 por el que se aplica el recurso plástico.
- **Ingresos 2026 verificados (EUR-Lex, Presupuesto General de la UE 2026, ingresos):** total €190.091M; desglose: RNB 70,28% (tasa 0,6930%), IVA 13,02% (tasa 0,30%), recursos propios tradicionales 11,24%, plástico 3,59%; bases IVA topeadas al 50% del RNB; retención estatal del 25% de los derechos de aduana (2021-2027).
- **Reforma en curso (propuesta, no derecho vigente):** paquete MFF 2028-2034 de la Comisión, 16-jul-2025 (COM(2025) 570/571): €1.763B en compromisos en precios 2025 (~1,26% del RNB, frente al 1,14% del marco 2021-2027); nuevos recursos propios propuestos: CBAM (régimen definitivo desde 2026), ETS, residuos de aparatos eléctricos no recogidos, impuesto especial sobre el tabaco, tasa e-commerce, ingresos ETIAS, retención aduanera 25%→10%, actualización del recurso plástico; estimación de ingresos adicionales ~€410.000M 2028-2035 (precios 2025); segundo paquete sectorial 3-sep-2025. Posición del PE: resolución 7-may-2025 y consenso amplio en la cámara por nuevos recursos propios, incluida la vía digital.
- **Multas del acervo digital (Comisión Europea):** Google Shopping €2.420M (2017; confirmado por el Tribunal General, 10-nov-2021), Android €4.340M (2018), AdSense €1.490M (2019), adtech €2.950M (sep-2025); primeras multas DMA (23-abr-2025): Apple €500M, Meta €200M. Las multas de competencia ingresan como «otros ingresos» del presupuesto de la UE (Consejo de la UE, «Financing the EU budget»).
- **Techos de sanción reales:** DSA, art. 52: hasta el 6% de la facturación mundial anual; AI Act, art. 99: hasta el 7% de la facturación mundial anual o €35M (el importe superior).
- **Precedentes de recursos no nacidos:** impuesto sobre transacciones financieras en cooperación reforzada (propuesta feb-2013, negociación estancada); gravamen digital europeo aparcado en 2021 a la espera del Pilar 1 de la OCDE, del que EE.UU. se retiró en enero de 2025; impuestos nacionales sobre servicios digitales vigentes en varios Estados miembros.
- **Marcos propios del libro:** Cap. 9B (ROI 164%, +€1.820M/año), Cap. 13 (protector puro: los cinco verbos), Cap. 14 (doble vía y consenso sobre exportación como posible recurso futuro), Cap. 15 (círculo recaudatorio y doctrina de la dotación), Cap. 17 (€2.600M/€3.400M; ecosistema 55.000-68.000 empleos).

Capítulo 17: Impacto Económico y Social del Poder Protector

La protección cognitiva como motor de prosperidad, empleo y liderazgo tecnológico europeo

Resumen del Capítulo

Este capítulo demuestra, con datos actualizados a julio de 2026, que el Poder Protector no es un gasto, sino la **inversión más estratégica de Europa en el siglo XXI**. Basado en estudios recientes de la **OCDE (2025-2026)**, **McKinsey (2026)**, **World Economic Forum (2026)**, **Comisión Europea (2026)** y **Eurostat (2026)**, se cuantifica su impacto: **empleo directo del PP según la trayectoria de dotación por etapas del Cap. 15** — ~3.000 en el núcleo (2035, escenario base), ~7.000-8.000 en el pleno (~2037) y más de 15.000 en la madurez 2040+—, **48.000-60.000 empleos indirectos en el escenario acelerado (55.000-68.000 empleos totales del ecosistema)**, **€7.200M-8.500M de impacto anual en el PIB**, y la creación de un ecosistema tecnológico europeo líder.

Tesis central: El Poder Protector no solo **protege la democracia**, sino que **genera prosperidad económica, atrae talento global y posiciona a Europa como líder en la era digital**. Cada euro invertido en protección cognitiva se multiplica entre **2,6x y 3,2x** en empleo, innovación y crecimiento, convirtiendo a la UE en un **imán para el talento y la inversión** en un sector con **CAGR del 13-20% anual**.

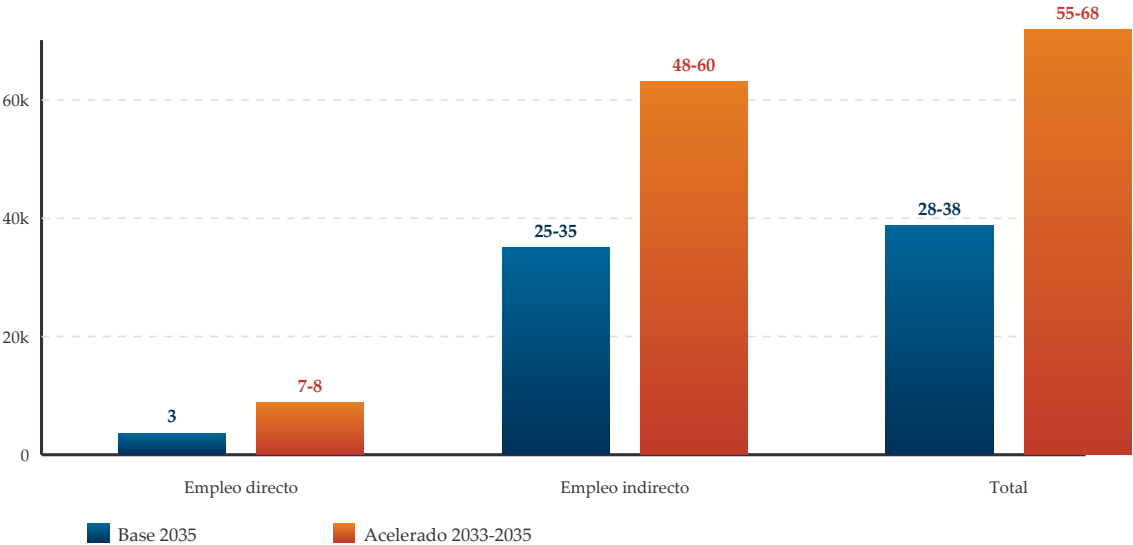
El Escenario Acelerado: la Respuesta a la Urgencia de 2026

Como se fundamenta en el **Capítulo 9**, la evidencia acumulada en 2026 —las alarmas de Bill Gates y Geoffrey Hinton, los 116.175 despidos atribuidos a la IA en EE.UU. entre enero y agosto, el 99% de los CEO que preparan recortes y una industria que modula sus advertencias según su cotización— obliga a **acelerar también el calendario del Poder Protector**. Si la EDSPA alcanza su plena capacidad operativa en **2028** (escenario acelerado del Capítulo 9), el Poder Protector puede lanzarse en **2029** y alcanzar sus hitos de referencia **dos años antes**.

A menos que se indique lo contrario, los datos de las secciones siguientes corresponden al **escenario base** (conservador). La tabla y los gráficos de esta sección presentan el **escenario acelerado recomendado**:

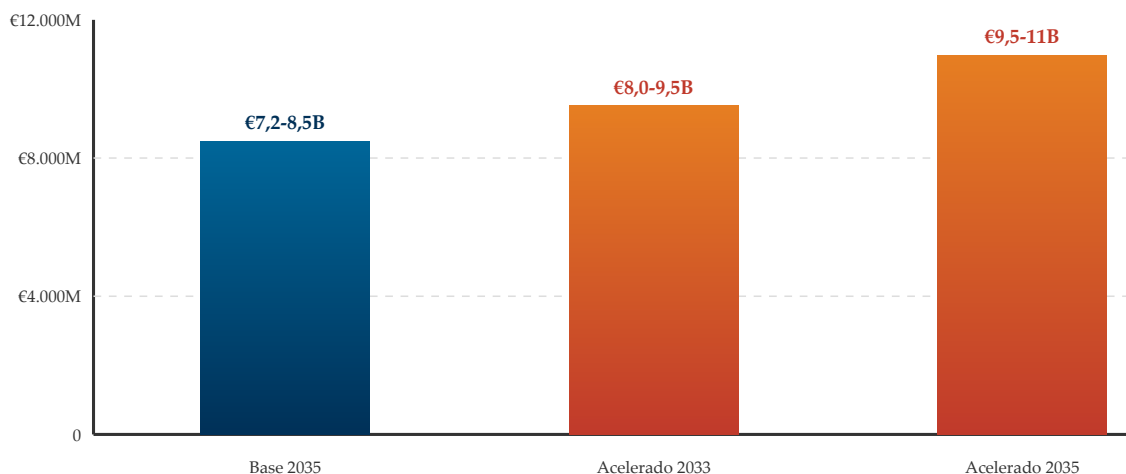
Métrica	Escenario Base	Escenario Acelerado (recomendado)
Lanzamiento del Poder Protector	2030 (reforma del Tratado 2032-2033)	2029: estructura preparatoria (financiada por el excedente anual de beneficios de la EDSPA) → firma del Tratado 2031-2032 → 2033: Poder Protector constitucional
Inversión inicial de arranque	€2.600M	€3.400M (2028-2029; prima de riesgo sistémico +30%, coherente con el Capítulo 9)
Empleo directo (hito)	~3.000 en 2035 (núcleo del PP, escenario base — Cap. 15)	~7.000-8.000 en 2035 (pleno: 27 Estados, 24 lenguas, 24/7) → >15.000 en la madurez 2040+
Empleo indirecto (hito)	25.000-35.000 en 2035	48.000-60.000 en 2035 → ecosistema total: 55.000-68.000 empleos
Impacto anual en el PIB (hito)	€7.200M-8.500M en 2035	€8.000M-9.500M en 2033 → €9.500M-11.000M en 2035
Impacto acumulado	€36.000M-42.500M (2035-2040)	€55.000M-65.000M (2033-2040) : mismos mecanismos, dos años más de generación
Fuga de cerebros	Pérdida de 5.000-7.000 expertos/año hasta 2035	Frenada en 2029-2030 (la EDSPA retiene talento); atracción neta desde 2031
Cuota de mercado global (2039)	40% Europa	45-50% : adelanto de la posición de referencia en estándares
Impacto por euro / Multiplicador	270-330% / 2,6x-3,2x	~250-300% / 2,6x-3,2x : el multiplicador es metodológico y no cambia; el ratio de impacto por euro baja por la mayor inversión, pero el beneficio absoluto es superior en ~€1.500M-2.000M/año

Empleo generado (miles de puestos) — escenario base 2035 vs. escenario acelerado



Miles de puestos de trabajo. Escenario base: hito en 2035. Escenario acelerado: hito en 2033 y valores superiores en 2035.

Impacto anual en el PIB (miles de millones €) — base vs. acelerado



Impacto anual en el PIB europeo. El escenario acelerado alcanza en 2033 el nivel que el base solo alcanza en 2035.

Nota de rigor institucional: se distingue la **estructura preparatoria** del Poder Protector (derecho derivado, acordable por cooperación reforzada: personal, infraestructura y capacidad técnica heredadas de la EDSPA, operativas desde 2029) de su **aprobación constitucional**, que exige Convención Europea, CIG unánime y ratificación por los 27 Estados miembros — un proceso históricamente no inferior a 4-5 años desde el lanzamiento político. La cronología acelerada (Convención 2029-2030, firma 2031-2032, entrada en vigor 2033) es la más rápida defendible, y solo es plausible porque la EDSPA habrá demostrado dos años de resultados medibles.

Coherencia financiera con el Capítulo 9: la estructura preparatoria de 2029 encaja con el punto de equilibrio acumulado de la EDSPA en **2028** (escenario acelerado, Capítulo 9 revisado). Los beneficios de la EDSPA financian parte de la inversión del Poder Protector (€2.600M base); la prima adicional de €800M del escenario acelerado queda cubierta con **menos de medio año del excedente anual de beneficios sobre costes de la EDSPA (~€1.960M/año a plena capacidad)**. Nota de rigor: no se trata de un «superávit estructural» — la EDSPA no es un negocio y no recauda; su aportación se contabiliza como valor económico generado (Capítulos 9 y 9B), no como ingreso presupuestario.

Contexto Macroeconómico Europeo (2026)

Los datos base de la UE (2026) muestran una economía en transformación digital acelerada, pero con desafíos clave:

€18,8B

PIB de la UE (billones)

221,2M

Empleo total UE (millones)

10,5M

Especialistas ICT en 2026 (objetivo:
20M en 2030)

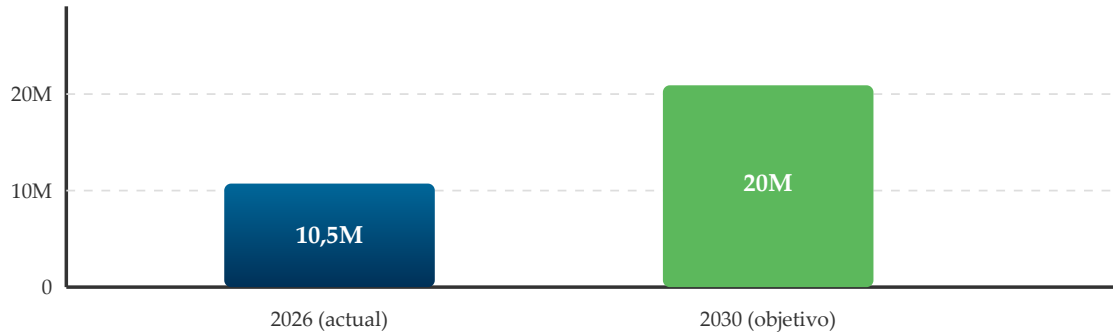
20%

Empresas que usan IA

€40.000M

Inversión en infraestructura digital
necesaria para 2030

Especialistas ICT: situación actual vs. objetivo europeo



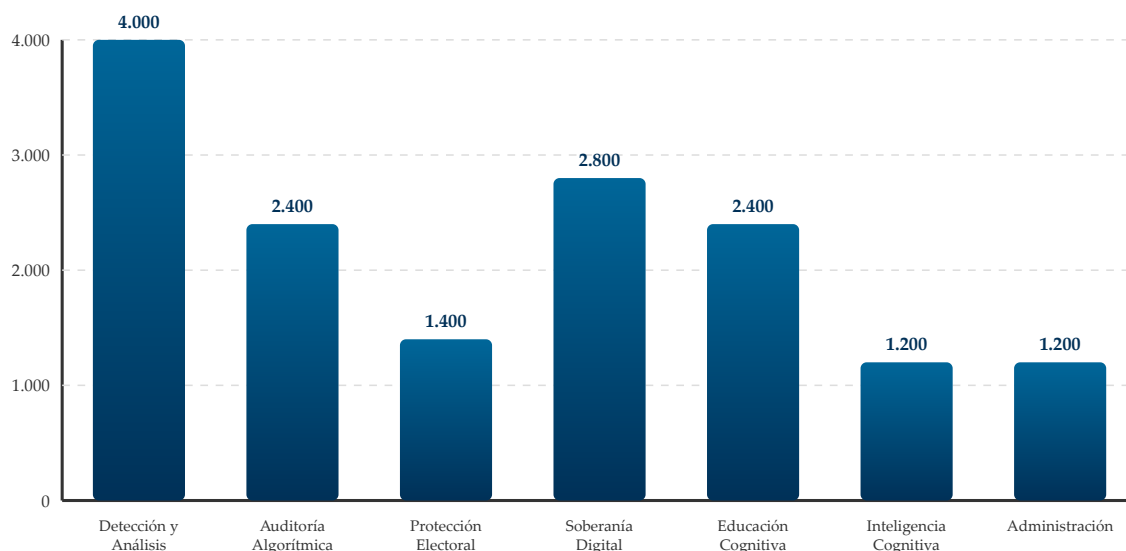
Contexto estratégico: La UE necesita **20 millones de especialistas ICT para 2030**, pero solo tiene **10,5 millones en 2026**. El **58% de los europeos** cambiarían a proveedores UE incluso a mayor coste (seguridad, protección de datos). Se necesitan **€40.000M** en infraestructura digital para 2030.

Sección 1: El Poder Protector como Generador de Empleo de Alta Calidad

1. Empleo Directo: la trayectoria de un poder — de los 1.500-2.000 de la EDSPA a más de 15.000 en madurez

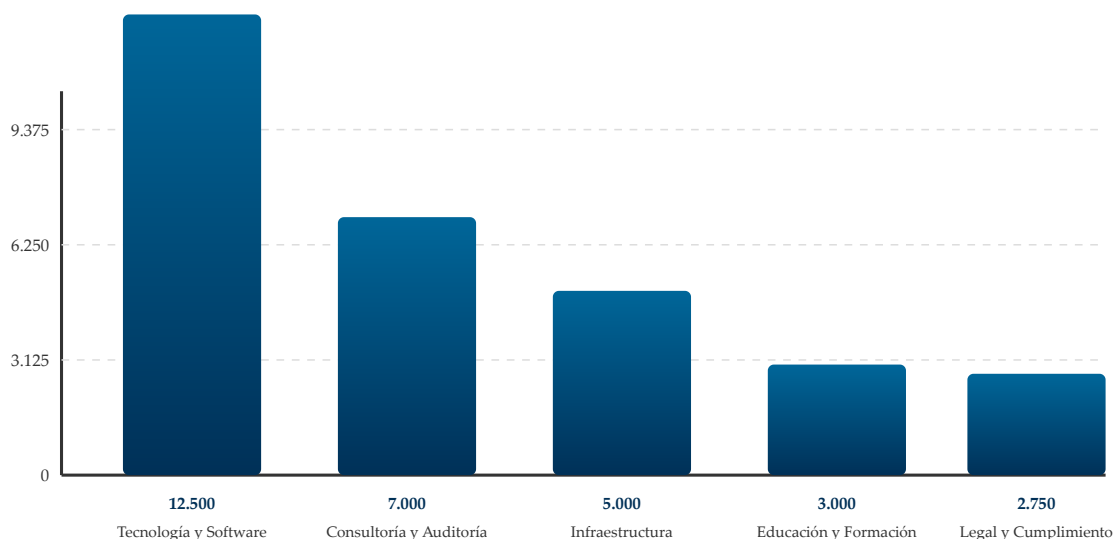
La estructura de personal del Poder Protector no es una plantilla fija: es la **trayectoria de dotación por etapas del Capítulo 15**, con disparadores contables (adhesiones de Estados, cobertura de la misión, volumen de amenaza, ampliaciones autorizadas por el legislador): **1.500-2.000 (EDSPA 2027-2030) → ~3.000 (núcleo 2033-2035) → ~7.000-8.000 (pleno ~2037: 27 Estados, 24 lenguas, 24/7) → más de 15.000 (madurez 2040+)**. Tres masas de personal la hacen inevitable: la escala real de la operación (con la doble verificación humano-IA del Cap. 8, deliberadamente no automatizable), el cuerpo de educación cognitiva (meta ≥90% en 2038) y el crecimiento orgánico de cometidos que acompaña a todo poder europeo — Frontex pasó de decenas de analistas a un cuerpo estatutario de 10.000 para 2027. El Comprobador Ciudadano del Cap. 13 está integrado en el horizonte de madurez, sin cifra propia. La distribución por áreas en la madurez (2040+):

Empleo directo del Poder Protector en madurez (2040+) — distribución por área (>15.000)



Nota de rigor: la distribución por áreas muestra la **madurez (2040+)**, no una plantilla de arranque: la dotación sigue la trayectoria por etapas del Capítulo 15 y cada salto tiene un disparador contable. La cifra no incluye el Comprobador Ciudadano del Cap. 13 (integrado sin cifra propia) y crece con las ampliaciones de cometidos que autorice el legislador. El empleo directo del PP es, por diseño, **el mayor polo europeo de empleo público del juicio humano no automatizable**: la doble verificación del Cap. 8 es un principio institucional, no una fase transitoria.

Empleo indirecto generado por el Poder Protector (escenario base 2035; 48.000-60.000 en el acelerado)



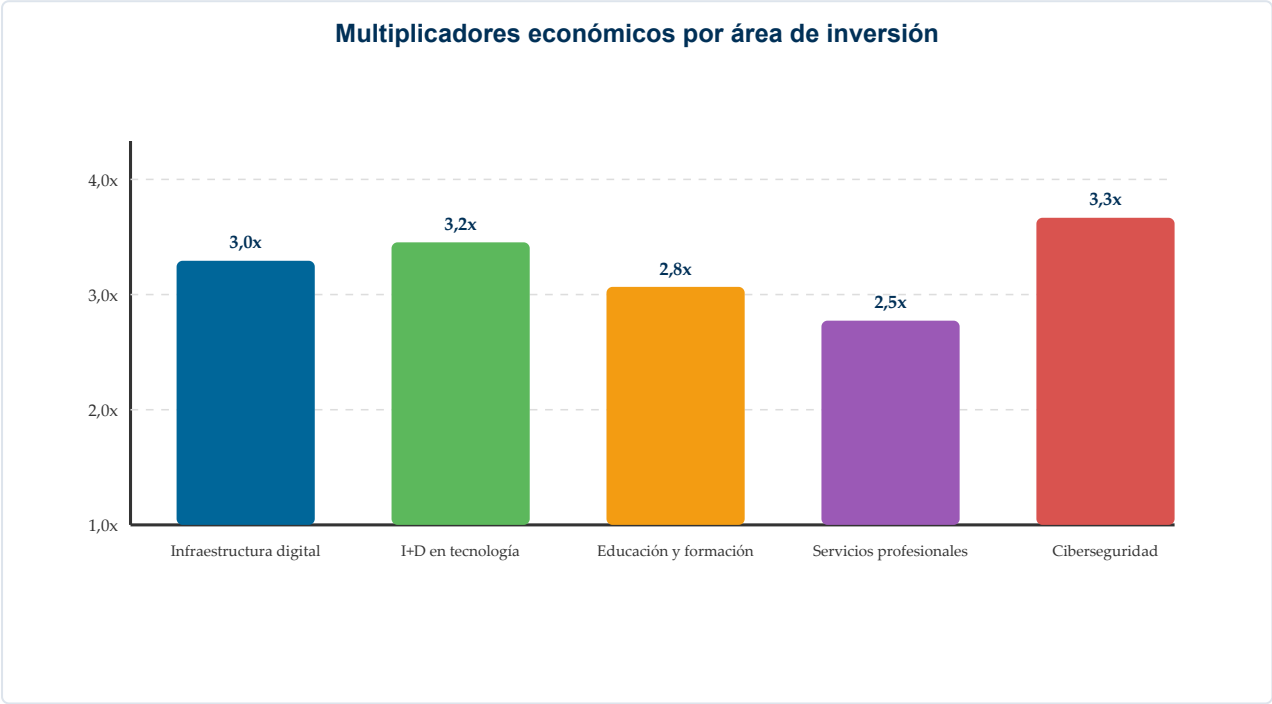
Efecto en el mercado laboral europeo (2026): Demanda de ciberseguridad en Europa: ~50% de las organizaciones. Crecimiento neto de contratación por IA en Europa: **+27% en 2026**. Habilidades más demandadas: Python (56%), IA/ML (47%), Java (34%), ciberseguridad (33%).

Sección 2: El Efecto Multiplicador Económico (2,6x-3,2x)

1. Metodología de Cálculo

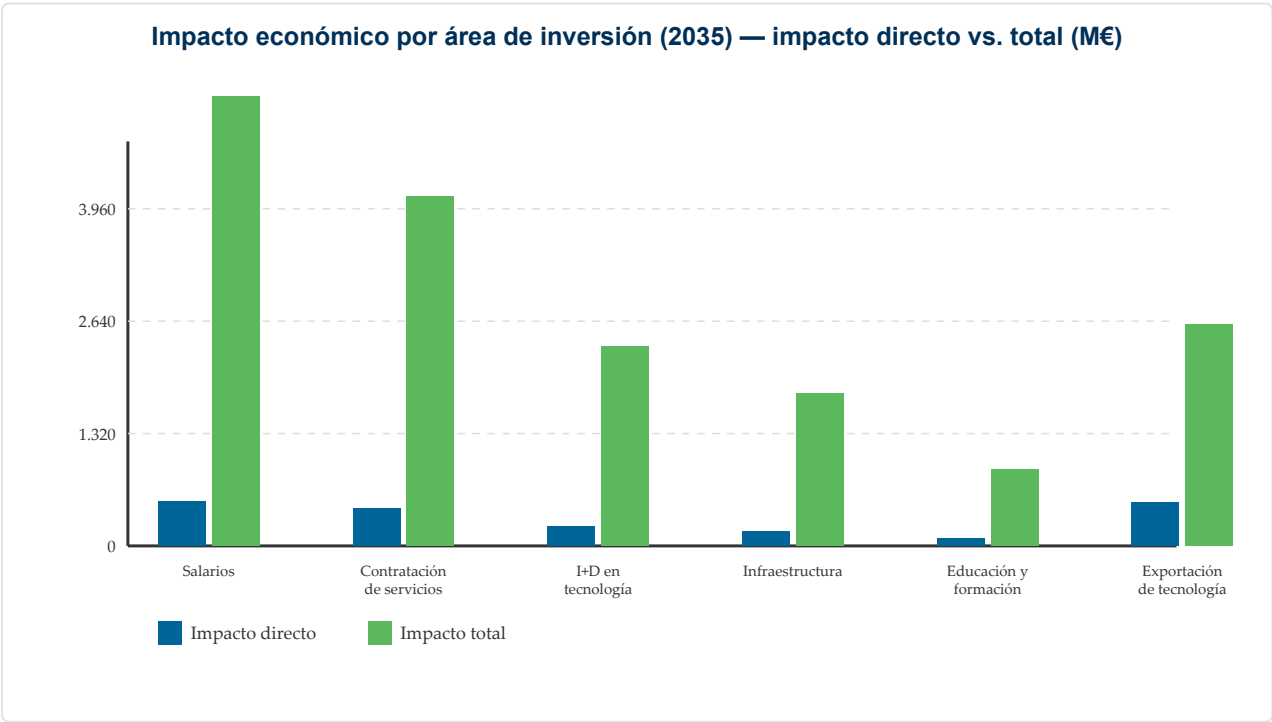
Basada en modelos Input-Output y multiplicador keynesiano:

- **Modelo Input-Output (Leontief):** Estimación del impacto en otros sectores.
- **Multiplicador Keynesiano:** $1/(1-MPC)$, donde $MPC \approx 0,6-0,7 \rightarrow$ Multiplicador $\approx 2,5x-3,3x$.
- **Validación empírica:** Mercado de ciberseguridad global (\$220B, CAGR 13%) $\rightarrow$ Multiplicador implícito: $\sim 3,0x$.



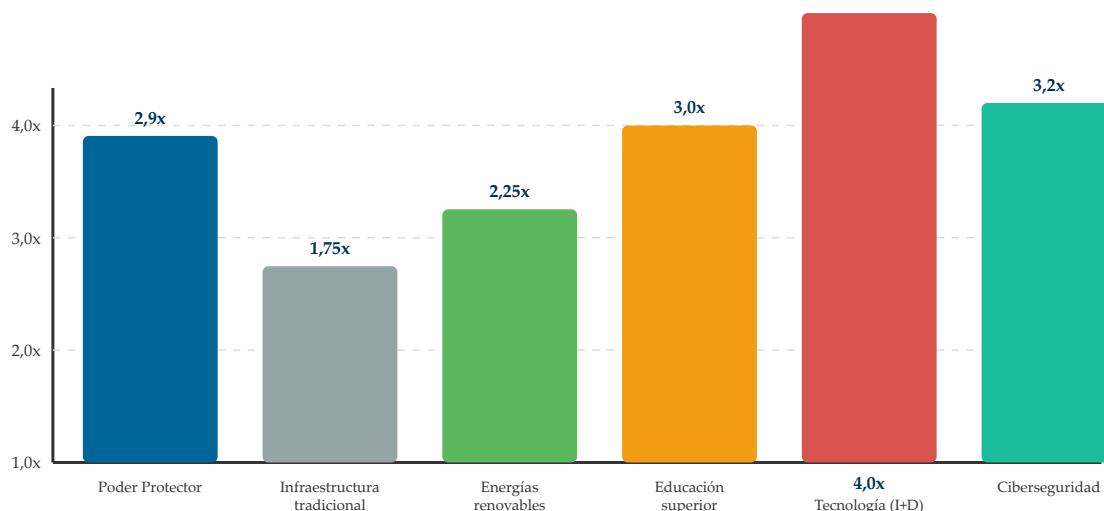
2. Análisis del Multiplicador por Área de Inversión

Desglose detallado del impacto económico del Poder Protector (2035):



Comparativa con otros sectores (2026):

Comparativa de multiplicadores económicos por sector

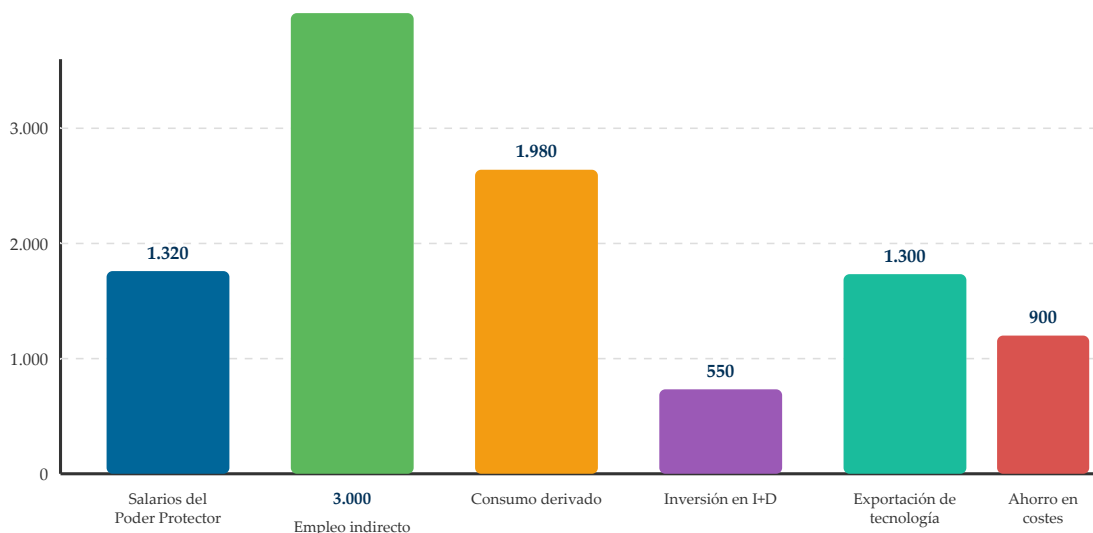


Sección 3: Impacto en el PIB Europeo (€7.200M-8.500M+ Anuales)

1. Cálculo del Impacto Directo e Indirecto

Desglose del impacto en el PIB (2035) — Metodología Input-Output:

Impacto en el PIB europeo por concepto (2035, M€)



Impacto acumulado (2035-2040): PIB adicional: €36.000M-42.500M (0,20%-0,23% del PIB de la UE). Empleo del ecosistema: 28.000-38.000 puestos (directos + indirectos) en el escenario base 2035; 55.000-68.000 en el acelerado. Crecimiento anual adicional: +0,04%-0,046% del PIB (equivalente a añadir el PIB de Chipre o Eslovenia cada año).

2. Comparativa con Otras Inversiones Públicas

Impacto por euro invertido y multiplicadores comparados:

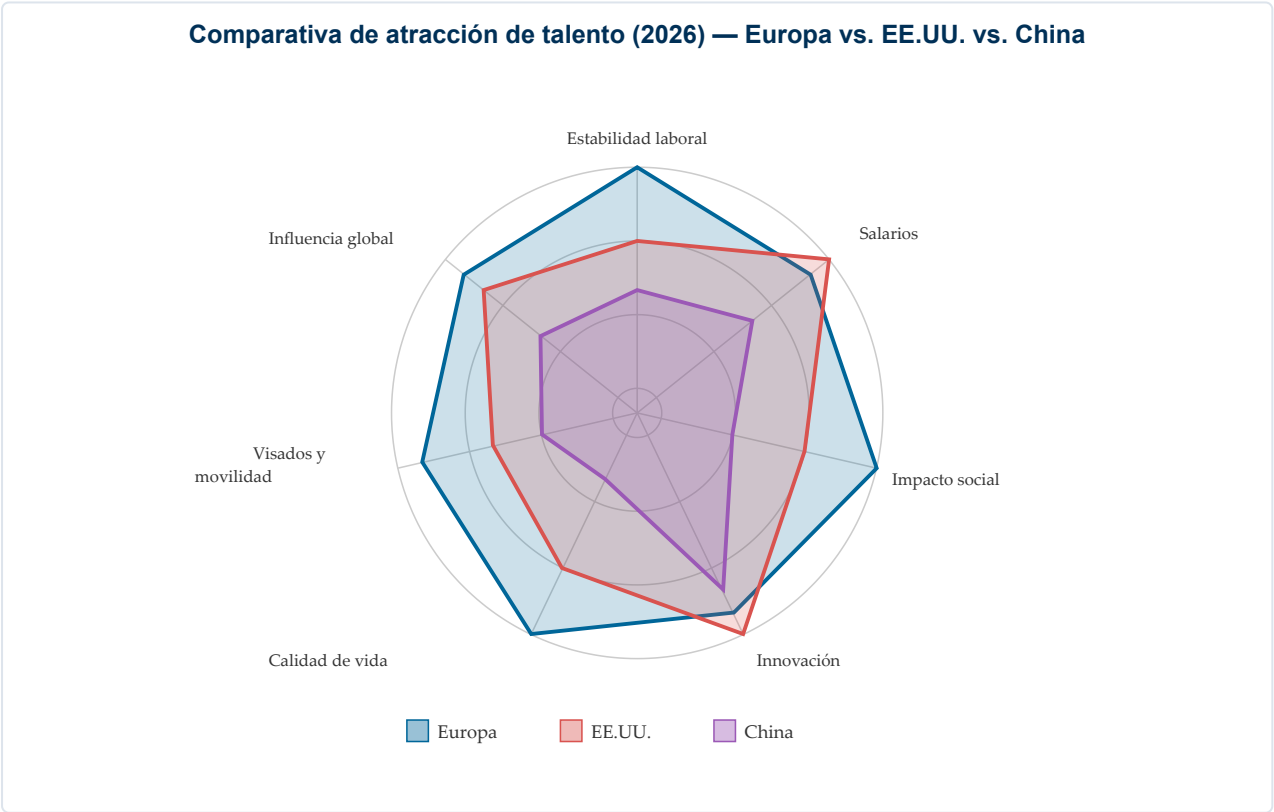
Inversión	Coste Anual	Impacto en PIB	Impacto por euro invertido	Multiplicador	Empleo Generado
Poder Protector	€2.600M-3.400M	€7.200M-8.500M	270-330%	2,6x-3,2x	55.000-68.000 (ecosistema, acelerado)
Horizon Europe (I+D)	€15.000M	€22.500M	150%	1,5x	200.000
Digital Europe Programme	€7.500M	€10.500M	140%	1,4x	50.000
Fondo NextGen	€800.000M	€1.200.000M	150%	1,5x	1.500.000
Ciberseguridad (UE)	€5.000M-10.000M	€15.000M-35.000M	300-500%	3,0x-3,5x	50.000-100.000

Conclusión: El Poder Protector tiene **uno de los mayores impactos por euro invertido** entre las inversiones públicas europeas, superando a programas como Horizon Europe (150%) o Digital Europe (140%). Su multiplicador (2,6x-3,2x) es comparable al de ciberseguridad (3,0x-3,5x) y superior al de infraestructura tradicional (1,5x-2,0x).

Sección 4: Atracción de Talento Global y Desarrollo del Ecosistema Tecnológico

1. El Poder Protector como Imán para Expertos Mundiales

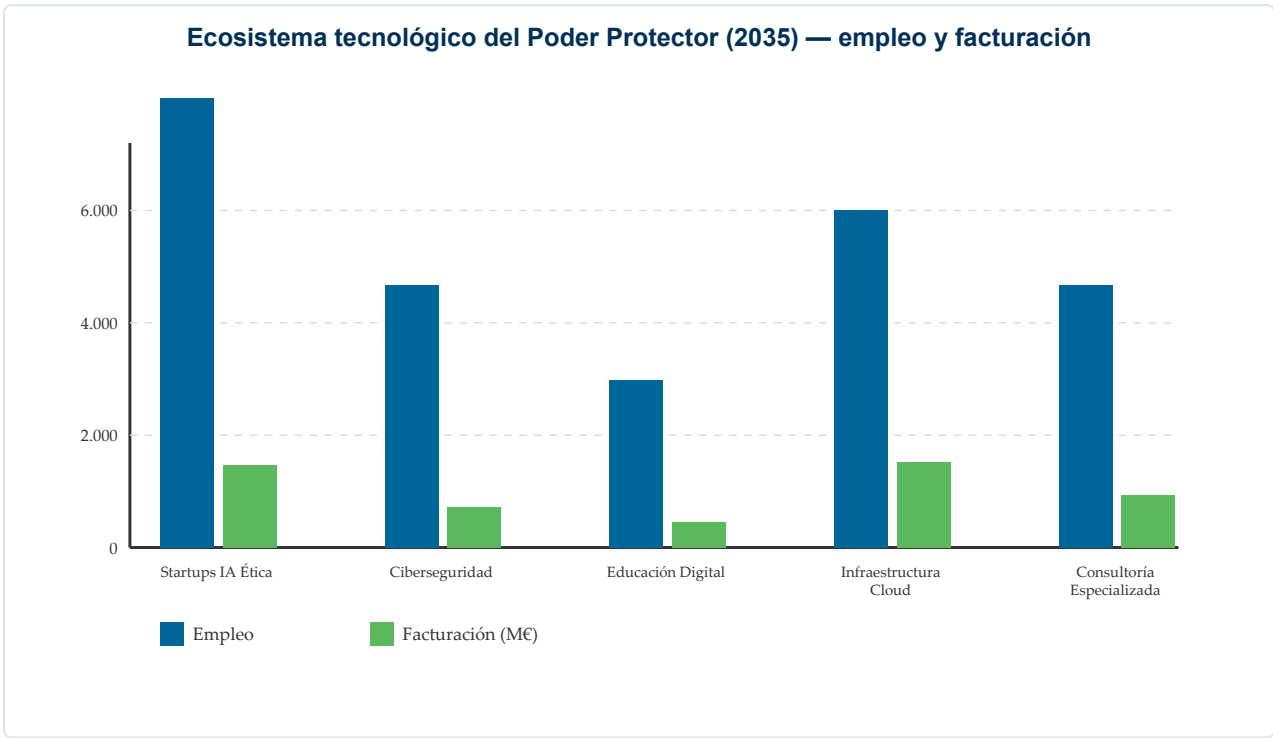
Comparativa de modelos de atracción de talento (2026), puntuación de 1 a 10:



Datos clave de atracción de talento (2026): Fuga de cerebros actual: Europa pierde 5.000-7.000 expertos en IA/año (hacia EE.UU. y China). Proyección con Poder Protector: **atracción neta de 2.000-3.000 expertos/año** (2035+). Países de origen de talento: EE.UU. (30%), Asia (25%), Latinoamérica (20%), África (15%), Europa del Este (10%).

2. Creación de un Ecosistema Tecnológico Europeo

Componentes del ecosistema (2035):



Beneficios del ecosistema (2026-2035):

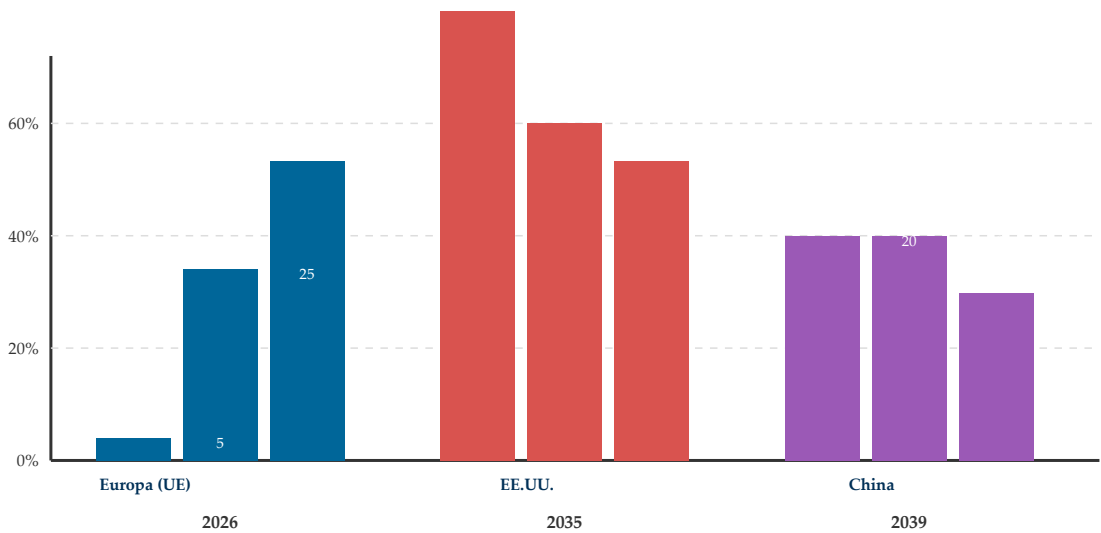
- Reducción de la dependencia tecnológica: 85% → <30% (2035).
- Creación de estándares globales: Europa como **referente en IA ética**.
- Atracción de inversión extranjera: **+20-30%** en startups de protección cognitiva.

Sección 5: Comparativa Internacional - Europa vs. EE.UU. vs. China

1. Tres Modelos de Control Digital en 2039

Cuota de mercado global en tecnología de protección cognitiva:

Cuota de mercado global en tecnología de protección cognitiva (%)

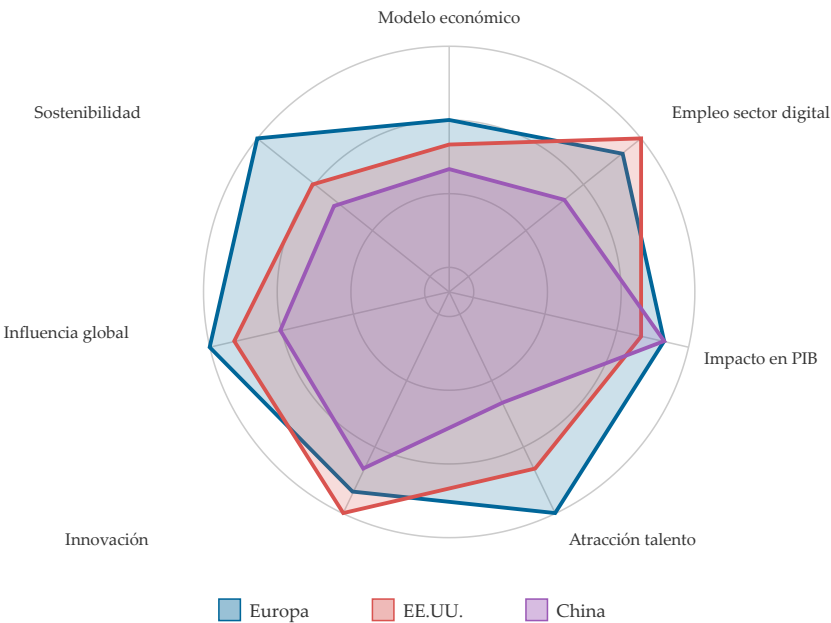


Razones del crecimiento europeo:

- **Modelo único:** Combina **tecnología avanzada** + **valores democráticos**.
- **Ecosistema integrado:** Poder Protector + startups + empresas + investigación.
- **Exportación de estándares:** La UE se convierte en **referente global**.
- **Atracción de talento:** Los mejores expertos **prefieren Europa**.

2. Comparativa Detallada de Modelos

Comparativa de modelos digitales (2039) — puntuación de 1 a 10

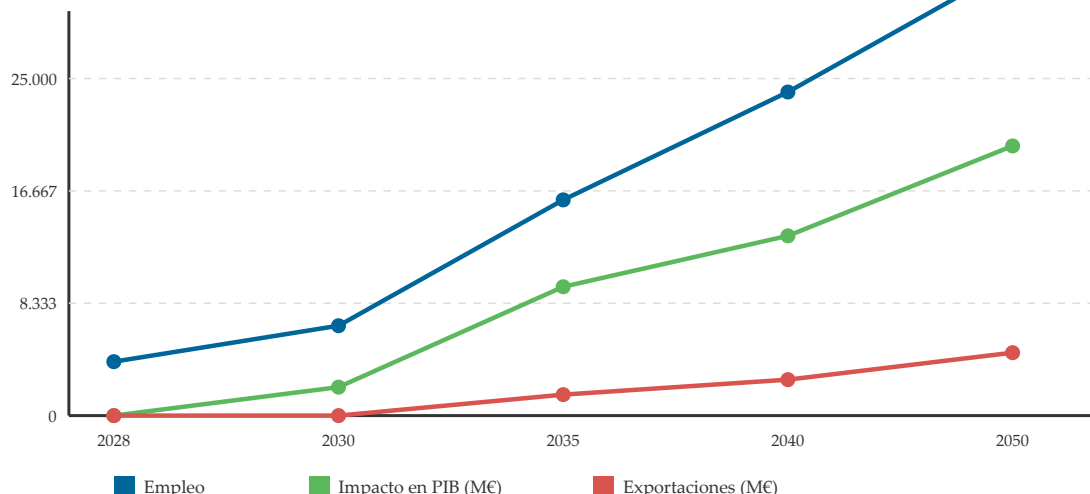


Mensaje clave: En 2039, mientras China celebra su centenario con un modelo de control digital autoritario, Europa presentará al mundo un modelo democrático de protección cognitiva basado en transparencia, derechos humanos y tecnología resiliente.

Conclusión: No Solo Protección, sino Prosperidad

El Poder Protector no es un gasto, sino la semilla de una nueva economía europea:

Evolución del impacto del Poder Protector (2028-2050)



"El siglo XXI será el siglo de quien controle la IA, controle el futuro."

Cinco razones por las que el Poder Protector cambiará Europa:

1. **Crea empleo de alta calidad** (28.000-38.000 empleos del ecosistema en el escenario base 2035; **55.000-68.000 en el escenario acelerado** — con la trayectoria de dotación del Cap. 15: ~3.000 directos en el núcleo → ~7.000-8.000 en el pleno ~2037 → **>15.000 en la madurez 2040+**, el mayor polo europeo de empleo público del juicio humano no automatizable frente a la IA).
2. **Genera crecimiento económico** (€7.200M-8.500M+ de impacto anual en el PIB en el escenario base; **€9.500M-11.000M en el acelerado**).
3. **Atrae al mejor talento del mundo** (Europa como imán para expertos en IA y ciberseguridad).
4. **Desarrolla un ecosistema tecnológico propio** (startups, empresas, centros de investigación).
5. **Exporta un modelo democrático** (Europa como referente global en protección cognitiva).

La ventana de decisión: la evidencia de 2026 (documentada en el Capítulo 9) indica que **el coste de esperar supera cada año a la prima de acelerar**. En el escenario acelerado, Europa alcanzaría en 2033 el nivel de empleo e impacto económico que el escenario base solo alcanzaría en 2035: **dos años de prosperidad y protección adicional** que no se recuperan después. Cada año de retraso es un año en que la fuga de talento continúa, la manipulación cognitiva avanza sin contrapeso y el mercado laboral se reorganiza sin red de protección.

La ecuación del éxito:

Protección cognitiva + Inversión pública + Ecosistema privado = Prosperidad europea + Liderazgo global

Visión a 2039: Europa no solo protege su democracia, sino que **la exporta al mundo**. El Poder Protector no es solo una institución para proteger a Europa, sino el motor que **la convertirá en la primera potencia digital democrática**.

tica del mundo. Mientras China celebra su centenario con un modelo de **control autoritario**, Europa presentará al mundo un modelo de **protección democrática** que cambiará el equilibrio de poder global.

Referencias verificadas

- **Datos macroeconómicos (Eurostat, 2026):** empleo total de la UE: 221,2 millones de personas (Q1-2026, ajustado estacionalmente); 20,0% de las empresas de la UE (10+ empleados) usaban tecnologías de IA (dato 2025, publicado en 2026); PIB de la UE: €18,8 billones (verificado en el Cap. 20).
- **Especialistas ICT (Década Digital, Decisión (UE) 2022/2481):** 10,4 millones de especialistas ICT empleados en la UE (2025), interpolados a ~10,5 millones en 2026; objetivo de 20 millones en 2030 (State of the Digital Decade).
- **Preferencias ciudadanas (Special Eurobarometer, Digital Decade 2026, trabajo de campo feb-mar 2026):** el 58% de los europeos cambiaría a un proveedor digital de la UE aunque costase algo más; el 85% respalda la inversión en infraestructura desarrollada en la UE.
- **Mercado de ciberseguridad:** ~\$220.000M globales con CAGR ~13% (Gartner: \$213.000M en 2025, ~\$240.000M proyectados 2026; MarketsandMarkets: \$219.000M en 2025, CAGR 13,8%); base de la validación empírica del multiplicador implícito ~3,0x.
- **Evidencia de urgencia 2026 (Cap. 9):** 116.175 despidos atribuidos a la IA en EE.UU. entre enero y agosto de 2026; alertas públicas de Bill Gates y Geoffrey Hinton; 99% de los CEO preparando recortes.
- **Marcos propios del libro:** Cap. 9 (escenarios base y acelerado), Cap. 9B (ROI neto del ecosistema: 164% a cinco años, +€1.820M/año), Cap. 13 (doble verificación humano-IA; Comprobador Ciudadano), Cap. 15 (trayectoria de dotación: 1.500-2.000 EDSPA → ~3.000 núcleo 2033-2035 → ~7.000-8.000 pleno ~2037 → >15.000 madurez 2040+; Frontex como precedente: 10.000 estatutarios para 2027), Cap. 16 (recursos propios: €2.600M base / €3.400M pleno).
- **Nota metodológica:** el multiplicador 2,6x-3,2x se estima con modelos input-output (Leontief) y el multiplicador keynesiano $1/(1-MPC)$, con $MPC \approx 0,6-0,7$. El «impacto por euro invertido» de las tablas (270-330% / 2,6x-3,2x) incluye efectos directos, indirectos e inducidos y no debe confundirse con el ROI neto del ecosistema (164%, Cap. 9B). El empleo indirecto (25.000-35.000 base / 48.000-60.000 acelerado, 2035) es estimación propia sobre multiplicadores de empleo del sector; las cuotas de mercado globales 2026-2039 y la atracción neta de talento (2.000-3.000 expertos/año desde 2035+) son proyecciones del escenario, no datos observados.

Capítulo 18: Tecnología e Infraestructura del Poder Protector

Resumen del capítulo

Este capítulo parte de una premisa que el libro entero comparte: **estamos construyendo algo que no existe, pero que es imprescindible** — la primera institución de la historia cuya función es proteger la esfera cognitiva de los ciudadanos frente a la manipulación industrial. Lo más importante no son las cifras: es la **seguridad del ciudadano**, que exige una institución fuerte, segura e independiente, con recursos propios. Y una institución así tiene una consecuencia tecnológica que ningún presupuesto anual puede esquivar: **quien protege la esfera cognitiva no puede depender de las herramientas de quien la manipula**. El diagnóstico está verificado y es brutal: el **80% de la infraestructura digital de Europa es importada** (informe EuroStack, Bertelsmann/Francesca Bria, 2025), y el experimento de soberanía-sello que fue Gaia-X enseñó la lección — la soberanía no se declara, se compra y se construye. Pero el terreno real de 2024-2026 ya no es el de hace tres años: JUPITER operó el primer superordenador exascale europeo (jun-2025), la UE seleccionó 13 fábricas de IA y lanzó la llamada oficial de gigafábricas (jul-2026) que moviliza más de **€30.000M**, e IRIS² (concesión firmada 16-dic-2024 por ~€10.550M y ~290 satélites; acuerdo de implementación del 7-ago-2026 que eleva el programa a €15.600M y 348 satélites, con despliegue desde 2029 y servicios gubernamentales ~2030) cita las campañas de desinformación entre sus amenazas declaradas. La arquitectura del capítulo construye sobre ese terreno con un modelo de **tres fases**: cliente ancla de lo existente (EDSPA 2027-2030) → primer Centro Forense Central propio (núcleo 2033-2035, capex plurianual separado del opex) → red propia ampliada y modelos propios (pleno ~2037 y madurez 2040+). Y lo dota de una pieza nueva: la **Cláusula de Aceleración Estratégica** — vigilancia continua, disparadores definidos, decisión en un máximo de 3 meses, inyección vía recursos propios (art. 311 TFUE) — porque el rival ya juega así: cuando le vetaron la litografía EUV, China construyó la propia, y su autosuficiencia en chips pasó del 16% (2024) al ~28% (finales de 2025). El capítulo cierra con el espejo que da urgencia a todo lo anterior: los **Dos Centenarios** de Xi Jinping tienen fecha — 2049, el centenario de la RPC — y la humanidad elegirá en esa fecha entre dos modelos terminados de gobernar la esfera cognitiva: el control autoritario o la verificación democrática. El Poder Protector es lo que hace que exista la segunda opción.

18.1 La premisa: lo que no existe y es imprescindible

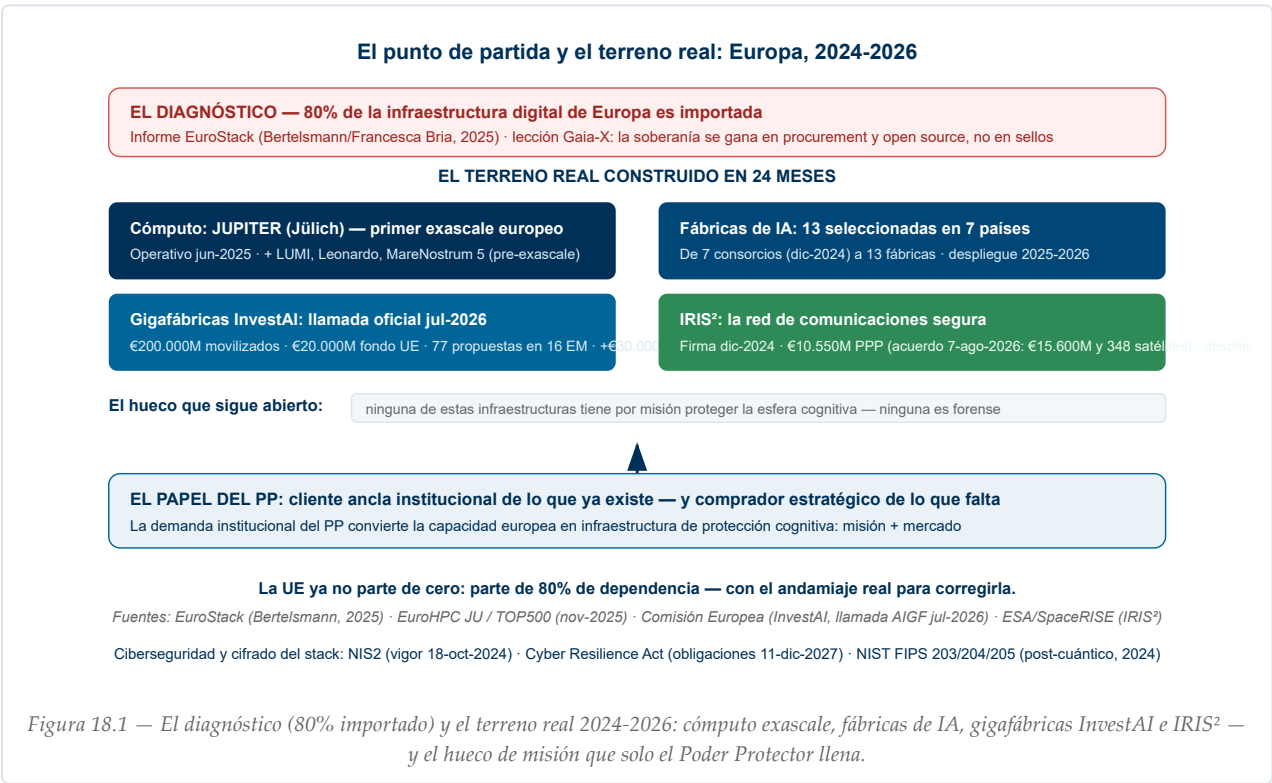
Ningún mercado produce lo que el Poder Protector compra, porque nadie ha tenido antes el cometido de proteger una esfera cognitiva. Ningún Estado autoritario lo producirá: la manipulación industrial es su instrumento de gobierno, no su amenaza. Y ninguna regulación reactiva basta: el DSA y el AI Act sancionan después del daño, con los medios forenses que las plataformas encauzadas les conceden. El hueco es exactamente el que el libro describe desde el Capítulo 1: **la esfera cognitiva es el único ámbito de la vida democrática que ningún poder protege** — y llenar ese hueco es, en sentido estricto, crear algo que no existe.

Crear lo que no existe tiene una regla técnica que este capítulo convierte en principio: la herramienta de protección no puede ser propiedad del protegido por manipular. Un escáner forense que corre en nube ajena audita con el permiso del auditado; un modelo que clasifica manipulación entrenado en silencio por terceros clasifica lo que el tercero quiere que clasifique. La institución del Capítulo 7 es fuerte, segura e independiente en lo jurídico; este capítulo es la condición para que lo sea también en lo técnico. Y una segunda regla, menos evidente y más ambiciosa: al dotarse de tecnología propia de protección cognitiva, **la Unión deja de ser cliente de la IA de otros y se convierte en agente estratégico de IA en la esfera cognitiva** — la verdadera necesidad de la humanidad para que las IA no se tornen dañinas sino beneficiosas: no basta con regularlas después; hay que demostrar, con infraestructura propia y verificación humana permanente, que la IA puede vivir bajo control democrático. La Unión que lo logre no habrá comprado un sistema: habrá producido el *modelo* civilizacional alternativo al control autoritario de la IA.

18.2 El diagnóstico verificado: 80% importado, Gaia-X y el terreno real

El punto de partida no admite maquillaje. El informe **EuroStack** (Bertelsmann Stiftung, coordinado por Francesca Bria, 2025) cifra en **80% la infraestructura digital de Europa que es importada**: del chip al modelo, del cable submarino al sistema operativo. Y el experimento más citado de soberanía digital europea — **Gaia-X** — enseña la lección de qué no hacer: una federación de estándares y sellos no desplaza a los proveedores dominantes si nadie compra; la soberanía se gana en la contratación pública (procurement) y en el código abierto, no en el certificado.

Pero el diagnóstico tiene una segunda mitad que el derrotismo omite: **el terreno real de 2024-2026 ya cambió**. JUPITER (Jülich) se convirtió en el primer superordenador **exascale** europeo — operativo en junio de 2025, el más rápido de Europa y cuarto del mundo en la lista TOP500 de noviembre de 2025— y se apoya en una constelación pre-exascale real: LUMI (Kajaani), Leonardo (Bologna), MareNostrum 5 (Barcelona). Sobre esa base, la política de fábricas de IA pasó de 7 consorcios (dic-2024) a **13 fábricas seleccionadas en 7 países**, en fase de despliegue durante 2025-2026. Y la escala dio otro salto con **InvestAI** (Cumbre de París, feb-2025): €200.000M movilizados con €20.000M de fondo europeo para gigafábricas de IA de ~100.000 aceleradores cada una; el Consejo adaptó el reglamento EuroHPC el 16-ene-2026 para incluirlas, la consulta informal recibió **77 propuestas en 16 Estados miembros (60 sitios)**, y la llamada oficial publicada en julio de 2026 desbloquea **más de €30.000M** de inversión. En el espacio, **IRIS²** (concesión firmada 16-dic-2024, consorcio SpaceRISE, ~€10.550M, 12 años, ~290 satélites desde 2029 — reforzada por el acuerdo de implementación del 7-ago-2026: €15.600M y 348 satélites) es la primera infraestructura europea que cita expresamente las campañas de desinformación entre las amenazas que debe resistir.



18.3 El principio operativo: tres fases, capex separado y la Cláusula de Aceleración Estratégica

La regla del capítulo es la contraria a la tentación de infraestructura por decreto: **usar lo que hay, comprar lo que falta y construir solo lo que nadie puede construir por la Unión** y hacerlo con una arquitectura financiera que el Capítulo 16 ya estableció: el **capex plurianual separado del opex anual**, dotado de recursos propios (art. 311 TFUE) y ejecutado por etapas.

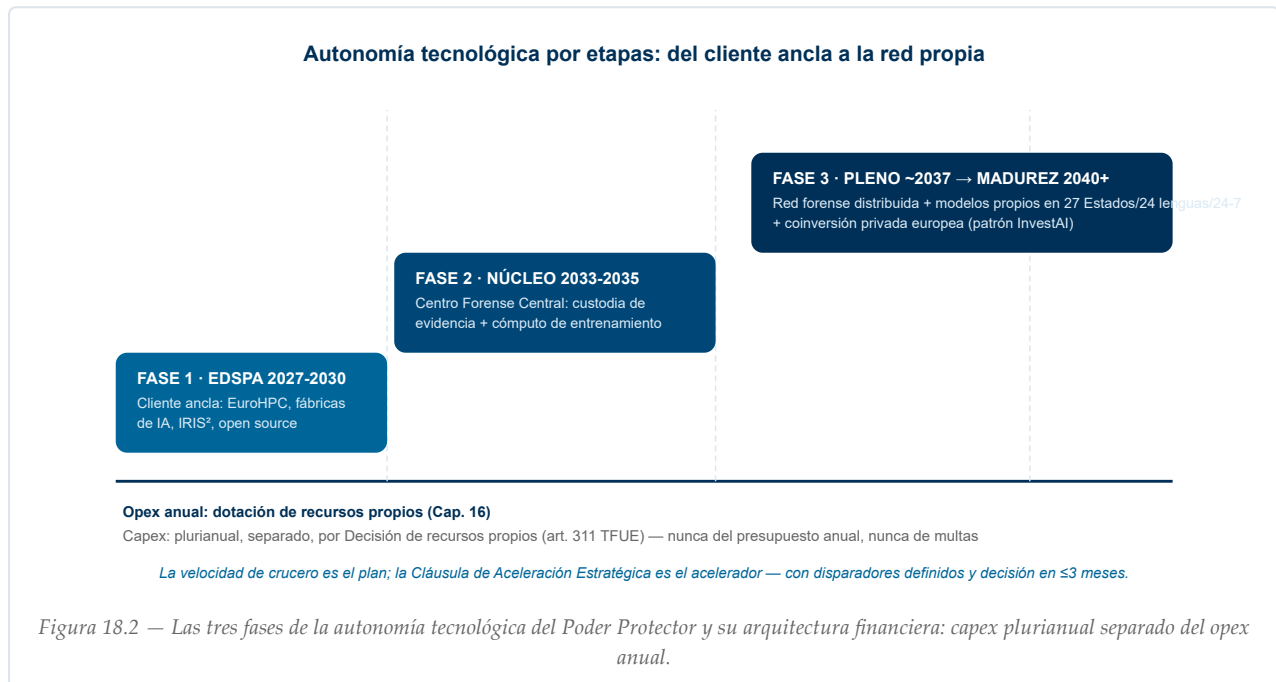
Las tres fases

Fase 1 — EDSPA como cliente ancla (2027-2030). La agencia no construye: alquila, compra y ancla. Cómputo en EuroHPC y fábricas de IA; servicios seguros sobre redes existentes e IRIS² cuando entre en servicio (~2029-2030); herramientas comerciales y de código abierto donde pasen la doble verificación del Cap. 8. Ser cliente ancla de la

capacidad europea es ya política tecnológica: la demanda institucional forense obliga a que la infraestructura europea sirva para proteger a los ciudadanos, no solo para competir en benchmarks.

Fase 2 — El núcleo construye (2033-2035). Con el Tratado en vigor, el PP levanta su primera pieza de propiedad institucional: el **Centro Forense Central** — custodia de evidencia (cadena de custodia certificada de materiales de manipulación, ejecutable y reproducible ante los tribunales) y cómputo de entrenamiento y auditoría para los modelos propios de la sección 18.4. El capex es plurianual, separado del opex de la dotación anual (Cap. 16), y su diseño sigue la lección de Gaia-X: procurement europeo y código abierto en cada capa donde exista alternativa creíble.

Fase 3 — Red propia y madurez (2037-2040+). El PP pleno (27 Estados, 24 lenguas, 24/7) opera una red forense distribuida conectada a IRIS², despliega sus modelos propios en toda la Unión y co-invierte con capital privado europeo siguiendo el patrón InvestAI: el Estado pone la misión y la demanda; el mercado europeo pone la escala. La exportación a democracias — el horizonte del Cap. 14/16 — nace de esta fase, sin cifras y sin supuestos.



La Cláusula de Aceleración Estratégica

La carrera tecnológica no respeta planes quinquenales, y el rival lo ha demostrado con el caso más citado de la década: cuando EE.UU. presionó para vetar la exportación de litografía EUV a China, **China construyó la alternativa propia** — SMIC fabricó el Kirin 9000s de 7nm sin EUV (Huawei Mate 60 Pro, ago-2023), SMEE entregó sus primeras litografías 28nm y solicitó patente EUV, Huawei lanzó los aceleradores Ascend (910C; serie 950 con HBM propia en 2026) y la autosuficiencia semiconductora china pasó del **16% en 2024 a ~28% a finales de 2025**, con ~\$150.000M de subsidios estatales y objetivos declarados de autosuficiencia en ascenso: el 70% original del plan Made in China 2025 y la nueva meta del 80% para 2030 (plan de 2026). El análisis de CSIS es inequívoco: los controles de exportación *aceleraron* la autosuficiencia china en lugar de frenarla. La lección para el diseño del PP no es copiar el autoritarismo: es **no ser la única potencia de la carrera que juega sin mecanismo de aceleración**.

Por eso el diseño dota al PP — y a la Unión — de un mecanismo institucional auditable, no de una chequera en blanco: la **Cláusula de Aceleración Estratégica**. Su diseño tiene cinco piezas:

1. **Velocidad de crucero por defecto.** El capex plurianual de las fases se ejecuta al ritmo planificado. Sin disparo, no hay aceleración: rigor presupuestario.
2. **Vigilancia estratégica continua.** El Departamento de Inteligencia Cognitiva (Cap. 12) mantiene un radar tecnológico con informe anual interno — el *Estado de la Carrera Cognitiva* — del que se publica **un resumen público sintético**: transparencia ante el ciudadano sin regalar al rival el mapa completo de lo que se vigila.
3. **Disparadores definidos a priori.** Cuatro disparadores duros activan la revisión extraordinaria; tres resortes suaves activan la revisión ordinaria (tabla siguiente). Definidos ahora, revisados anualmente, jamás improvisados bajo presión.

4. **Decisión en un máximo de 3 meses.** El disparo abre una revisión extraordinaria del capex que debe concluir en decisión en un trimestre — en la era digital, doce meses es una eternidad; los procedimientos urgentes reales de la UE se miden en semanas-meses, y la protección de la esfera cognitiva no puede esperar al ciclo presupuestario anual.
5. **Inyección vía recursos propios.** La aceleración se financia siempre por la vía del art. 311 TFUE (Cap. 16): nunca con presupuesto a cargo de las multas del PP, nunca como ingreso propio del poder que detecta — el protector puro queda intacto también aquí.

Disparador / resorte	Naturaleza	Respuesta
D1 · Veto tecnológico a la UE — cualquier actor que bloquee acceso a cómputo, chips, modelos o infraestructura crítica para el PP	Duro	Revisión extraordinaria del capex; decisión ≤3 meses; inyección vía art. 311 TFUE
D2 · Salto cualitativo verificado en IA de manipulación — capacidad de manipulación cognitiva masiva que el Escáner forense no pueda caracterizar con fiabilidad	Duro	Revisión extraordinaria del capex; decisión ≤3 meses; inyección vía art. 311 TFUE
D3 · Brecha de cómputo estratégica — la capacidad de cómputo soberana de la UE cae por debajo del umbral relativo fijado reglamentariamente frente a un rival	Duro	Revisión extraordinaria del capex; decisión ≤3 meses; inyección vía art. 311 TFUE
D4 · Interdependencia crítica detectada — una parte esencial de la cadena del PP depende de un solo proveedor o de una jurisdicción no europea	Duro	Revisión extraordinaria del capex; decisión ≤3 meses; inyección vía art. 311 TFUE
S1 · Sobrecarga operativa — asuntos sostenidos por encima del umbral (cláusula de escalado del Cap. 12, >150-200 asuntos/año)	Suave	Revisión ordinaria del capex en el ciclo plurianual siguiente
S2 · Cuadro de mando de soberanía — auditoría anual de cadena de suministro: % de componentes europeos por capa (Fig. 18.3)	Suave	Informe al Consejo y al PE; planes de corrección por capa
S3 · Ejercicio de estrés anual (red team) — simular el corte total de dependencias externas y medir la resiliencia del PP (estilo pruebas de resiliencia bancaria)	Suave	Hallazgos al resumen público sintético; alimentación continua de D1-D4

Umbrales y arquetipos — cómo se dispara en la práctica: el texto fija los disparadores por definición institucional; sus *umbrales exactos* (p. ej. la magnitud de la brecha de cómputo de D3) se establecerían por reglamento del Consejo a propuesta del PP, revisados anualmente con el informe *Estado de la Carrera Cognitiva*. A título ilustrativo del funcionamiento del mecanismo, estos serían arquetipos de disparo, calibrados con casos reales 2024-2026: un veto a la exportación de aceleradores de IA a la Unión (el precedente del veto EUV a China, 2019/2023) dispararía D1; una IA de manipulación que supere al Escáner forense en un orden de magnitud dispararía D2; y la trayectoria china 16%→28% de autosuficiencia en 18 meses (~\$150.000M de subsidios; Ascend 950 con HBM propia, 2026) muestra la velocidad a la que un rival puede cerrar una brecha — y por tanto la velocidad a la que el radar debe detectarla. El plazo de decisión de ≤3 meses es una propuesta de diseño institucional de este libro, alineada con la escala temporal real de los procedimientos urgentes de la Unión, no una norma existente.

18.4 IA propias por requisito: el Escáner forense y las herramientas del Auditor y del Educador

El corazón tecnológico del PP no es una lista de productos: son **tres herramientas nucleares definidas por requisito institucional**, la primera de las cuales ya existe desde el Capítulo 8. Sus nombres son funcionales y deliberadamente sobrios, y ninguna se define por parámetros de modelo — eso lo decide el procurement y el estado del arte, no un libro:

- **El Escáner forense cognitivo** (Cap. 8): el instrumento de detección y caracterización de la manipulación — no un árbitro de la verdad. Su requisito nuclear: que su evidencia sea **reproducible ante los tribunales**, con cadena de custodia certificada (Centro Forense Central, Fase 2) y doble verificación humano-IA en todo hallazgo.
- **El instrumental del Auditor** (Cap. 13): herramientas de auditoría algorítmica de sistemas de recomendación, publicidad y moderación de las plataformas — acceso a datos de investigador (DSA, art. 40) convertido en escrutinio sistemático, con modelos capaces de explicar *por qué* un sistema amplifica o entierra, no solo de medir que lo hace.
- **El instrumental del Educador** (Cap. 13): la capa que adapta la evidencia del Escáner a ciudadanía, escuelas y profesionales — diagnóstico de vulnerabilidad cognitiva a escala (el Kit del Cap. 2 en positivo), currículos y

simulacros verificables en 24 lenguas.

Las tres comparten un mismo contrato de requisito, y este es el punto donde el capítulo conecta con la premisa de 18.1: **abiertas, auditables y explicables** — código abierto donde exista alternativa creíble, auditoría pública de sus componentes, explicabilidad de cada hallazgo, y la doble verificación humano-IA del Cap. 8 como condición de uso. Ninguna de las tres puede ser una caja negra, porque el poder que las usa no puede serlo. El Escáner que certifica manipulación con método secreto es un oráculo, no una institución; y el PP del libro es deliberadamente lo contrario: **el lugar donde la IA se somete, por primera vez y con medios propios, a verificación democrática permanente**. Ahí — no en los parámetros de ningún modelo — está la apuesta civilizacional: demostrar que una comunidad de ciudadanos libres puede tener inteligencia artificial bajo su control, y que esa es la única base sobre la que la humanidad puede hacer que la IA no se torne dañina sino beneficiosa.

El cuadro de mando de soberanía (S2): auditoría anual de dependencia por capa

Cada capa del stack del PP, auditada anualmente: ¿de quién depende?

Cómputo (Fase 1: EuroHPC/fábricas de IA → Fase 2: Centro Forense Central)

 hoy: dependencia alta (80% importado, EuroStack)

Modelos (Fase 1: open source verificado → Fase 3: modelos propios)

 en transición: bases abiertas + herramientas propias por requisito

Red y comunicaciones (Fase 1: comerciales/IRIS² desde ~2030)

 en transición: IRIS² gubernamental ~2030 → red forense Fase 3

Custodia de evidencia (Fase 2: Centro Forense Central — propiedad institucional)

 bajo control: jurisdicción y cadena de custodia europeas

Talento y metodología (Cáp. 7-8: >15.000 en madurez 2040+, doble verificación humano-IA)

 bajo control: el activo que ninguna exportación controla

Objetivo del cuadro de mandos: que el rojo y el naranja se vuelvan verdes por capa — con fechas, proveedor alternativo y coste

Esquema de diseño del mecanismo S2 (no cifras de estado actual): la auditoría anual mide la dependencia real por capa y la publica en el resumen sintético.

El único dato cuantificado del punto de partida es el 80% importado (EuroStack, 2025) — el resto lo mide la auditoría cuando el PP existe.

Figura 18.3 — El cuadro de mando de soberanía del resorte S2: la auditoría anual que convierte «80% importado» en un plan medible capa a capa.

18.5 El espejo de 2049: los Dos Centenarios y la carrera por la esfera cognitiva

Toda estrategia seria tiene fecha, y la del rival está publicada desde 2012: en el XVIII Congreso del Partido, Xi Jinping fijó los **Dos Centenarios** — la sociedad xiaokang para 2021 y, para **2049, centenario de la República Popular China, un «país socialista moderno, próspero y fuerte»** — con hito intermedio en 2035 y su anexo tecnológico, China Standards 2035. La estrategia de IA del rival también tiene su doctrina explícita: en la sesión del Politburó de abril de 2025, Xi exigió IA «independiente y controlable» (自主可控) y autosuficiente (自立自强), y el XV Plan Quinquenal (2026-2030) convirtió la autosuficiencia en semiconductores e IA en proyecto nacional generacional. Nada de esto es una profecía de este libro: son compromisos públicos con calendario del adversario. **El rival tiene estrategia a 100 años; las democracias no tienen ni estrategia ni fecha.**

El Poder Protector da a Europa las dos cosas que le faltan. Una estrategia: la protección de la esfera cognitiva como misión permanente, con infraestructura propia y mecanismo de aceleración. Y una fecha de contrapeso: **el PP pleno hacia ~2037, madurez hacia 2040+** — simétrico del hito intermedio chino de 2035, y a tiempo para que en 2049 la Unión no llegue descabezada al centenario del rival. En 2049 el mundo no elegirá entre dos velocidades de progreso: elegirá entre **dos modelos terminados de gobernar la esfera cognitiva** — el control autoritario, donde la IA es instrumento del poder, y la verificación democrática, donde la IA vive bajo control ciudadano permanente. Este libro no profetiza quién gana. Pero sí afirma, en ambas direcciones, lo que la historia de este capítulo hace evidente: **si no existe el segundo modelo, la elección de 2049 no será una elección**. Y si existe — maduro, verificado y operativo hacia 2040+ —, el modelo europeo de IA protectora de la esfera cognitiva será **el referente estratégico de todas las democracias del mundo**: toda democracia que enfrente la manipulación industrial — Estado, bloque u organización democrática — necesitará exactamente lo que el PP ya habrá construido: escáner forense reproducible ante los tribunales, auditoría algorítmica explicable, educación cognitiva a escala y la demostración verificada de que la IA puede servir a la libertad en lugar de domesticarla. Ese es el sentido geopolítico último de la exportación del Cap. 14/16 — sin cifras, pero sin falsa modestia: **quien tenga el modelo pro-**

tector terminado no será un actor más en 2049; será el referente al que las democracias mirarán, como quien controle el modelo autoritario será el referente al que mirarán los autócratas. Europa puede llegar a 2049 siendo cliente de la IA de otros — o siendo la democracia que produjo el modelo de IA protectora de la esfera cognitiva. El Poder Protector es lo que hace que exista la segunda opción — y la carrera que hay que ganar es, literalmente, por la libertad de la humanidad.

18.6 Conclusión

1. **La premisa.** El PP es algo que no existe y es imprescindible: la primera institución que protege la esfera cognitiva del ciudadano. Su requisito tecnológico no es tener cifras grandes: ser fuerte, seguro e independiente — lo que implica no depender de las herramientas de quien manipula.
2. **El diagnóstico es doble.** 80% de la infraestructura digital de Europa es importada (EuroStack) y Gaia-X enseña que la soberanía no se declara — pero el terreno real de 2024-2026 (JUPITER exascale, 13 fábricas de IA, gigafábricas InvestAI con llamada oficial en jul-2026 por +€30.000M, IRIS² desde 2029) es el andamiaje real sobre el que el PP construye.
3. **Tres fases, capex separado.** Cliente ancla (2027-2030) → Centro Forense Central propio (2033-2035) → red propia y modelos propios (pleno ~2037, madurez 2040+), con capex plurianual vía art. 311 TFUE, jamás capex fantasma por decreto.
4. **La Cláusula de Aceleración Estratégica.** Crucero por defecto, radar anual con resumen público sintético, 4 disparadores duros + 3 resortes suaves definidos a priori, decisión en ≤3 meses, inyección vía recursos propios — porque el rival ya juega así: al vetarle la litografía EUV, construyó la propia y pasó del 16% al 28% de autosuficiencia en 18 meses.
5. **IA por requisito, no por parámetros.** Escáner forense cognitivo, instrumental del Auditor e instrumental del Educador: abiertos, auditables, explicables, con doble verificación humano-IA — el PP como el lugar donde la IA se somete a verificación democrática permanente.
6. **El espejo de 2049.** Los Dos Centenarios del rival tienen fecha pública; el PP da a Europa estrategia y fecha de contrapeso (pleno ~2037, madurez 2040+). Sin profecía de victoria — pero con relevancia ganada a pulso: si el modelo madura, el PP convierte a Europa en el referente estratégico de las democracias del mundo y en exportadora del modelo de IA protectora de la esfera cognitiva (horizonte del Cap. 14/16, sin cifras).

La tesis del capítulo en una frase: no se protege la esfera cognitiva con las herramientas de quien la manipula — el Poder Protector construye su autonomía por etapas sobre el terreno real europeo, se dota de un mecanismo auditable de aceleración porque el rival ya corre con fecha (2049), y convierte a la Unión en el único lugar del mundo donde la inteligencia artificial rinde cuentas, con medios propios, ante el ciudadano.

18.7 Fuentes y referencias verificadas

- **Diagnóstico europeo:** informe EuroStack (Bertelsmann Stiftung, coordinado por Francesca Bria, 2025): 80% de la infraestructura digital de Europa importada; lección Gaia-X (soberanía vía procurement y open source).
- **Cómputo europeo:** EuroHPC JU: JUPITER (Jülich), primer superordenador exascale europeo, operativo jun-2025 (1ª posición europea y 4ª mundial, TOP500 nov-2025); LUMI (Kajaani), Leonardo (Bolonía), MareNostrum 5 (Barcelona) pre-exascale.
- **Fábricas y gigafábricas de IA:** 7 consorcios seleccionados dic-2024 (15 EM) → 13 fábricas de IA en 7 países (2025), en despliegue 2025-2026; InvestAI (Cumbre de París, 11-feb-2025): €200.000M movilizados, €20.000M de fondo UE para 4-5 gigafábricas de ~100.000 aceleradores; Consejo de la UE, 16-ene-2026: reglamento EuroHPC (Reg. 2021/1173, mod. Reg. 2026/150) adaptado para incluir gigafábricas; consulta informal: 77 propuestas en 16 EM / 60 sitios (jun-2025); llamada oficial jul-2026 con más de €30.000M en inversión (Comisión Europea).
- **IRIS²:** concesión firmada 16-dic-2024 (consorcio SpaceRISE), PPP de 12 años, ~€10.550M y ~290 satélites (despliegue desde 2029, servicios gubernamentales ~2030); acuerdo de implementación del 7-ago-2026 (Comisión/ESA/SpaceRISE) que eleva el programa a €15.600M y 348 satélites; las campañas de desinformación figuran entre sus amenazas declaradas.
- **Ciberseguridad y cifrado:** Directiva NIS2 (en vigor 18-oct-2024); Cyber Resilience Act (notificación 11-sep-2026, obligaciones 11-dic-2027); ENISA; post-cuántico: NIST FIPS 203/204/205 (2024), hoja de ruta de transición (depreciación RSA/ECC 2030, prohibición 2035, IR 8547).

- **El caso del rival (Chip War):** veto de exportación de litografía EUV a China bajo presión de EE.UU. (2019/2023); Huawei Mate 60 Pro (ago-2023) con Kirin 9000s 7nm de SMIC fabricado sin EUV; SMEE: primeras litografías 28nm (finales de 2023) y patente EUV (mar-2023); Huawei Ascend 910C (60-80% del rendimiento NVIDIA en inferencia) y serie Ascend 950 con HBM propia (Q1 2026); autosuficiencia semiconductora china 16% (2024) → ~28% (Q4 2025), ~\$150.000M en subsidios, metas declaradas: 70% del plan Made in China 2025 (no alcanzada) y 80% para 2030 (plan de 2026) (CSIS; Huawei/Ren Zhengfei ante Xi, feb-2025); análisis CSIS: los controles aceleraron la autosuficiencia china; sesión del Politburó (abr-2025): Xi exige IA «independiente y controlable» (自主可控) y autosuficiente (自立自强); XV Plan Quinquenal (2026-2030): autosuficiencia en semiconductores e IA como proyecto nacional generacional.
- **Los Dos Centenarios:** formulados por Xi Jinping en el XVIII Congreso del PCC (2012): sociedad xiaokang para 2021 y país socialista moderno para 2049 (centenario de la RPC), con hito intermedio 2035 y China Standards 2035.
- **Autoritarismo digital exportado:** Ruta de la Seda Digital (informes CNAS): exportación del modelo de vigilancia y control a África, Asia Oriental y América Latina.
- **Marcos propios del libro:** Cap. 7 (estructura y Departamento de Inteligencia Cognitiva), Cap. 8 (Escáner forense cognitivo, doble verificación humano-IA), Cap. 12 (cláusula de escalado >150-200 asuntos/año; Dpto. Soberanía Digital), Cap. 13 (cinco verbos; auditoría algorítmica; educación), Cap. 14 (doble vía constitucional; exportación como horizonte sin cifras), Cap. 15 (trayectoria de dotación >15.000 en madurez 2040+), Cap. 16 (recursos propios art. 311 TFUE; capex separado del opex), Cap. 17 (ecosistema 55.000-68.000 empleos).

Capítulo 19: Estrategia de Comunicación del Poder Protector

Resumen del capítulo

Un poder constitucional no se comunica como se comunica un producto: se comunica como se comunica una confianza. La tesis de este capítulo es que la comunicación del Poder Protector no es marketing añadido: es **la función institucional que cierra el círculo de la legitimidad** — porque un poder que protege la esfera cognitiva sin que el ciudadano pueda verlo, verificarlo y entenderlo no existe políticamente. El punto de partida es una paradoja verificada que este capítulo convierte en su eje: los europeos están más preocupados que nunca por la desinformación (69% la considera un problema en el Eurobarómetro de 2026, hasta 85% en España) y al mismo tiempo una mayoría (60% en el Trust Survey de la OCDE 2026) desconfía del uso gubernamental de la IA. La protección que exigen y la herramienta que la haría posible generan, hoy, la misma desconfianza. Esa paradoja no es un obstáculo del PP: es **exactamente el problema que el PP fue diseñado para resolver** — es la única institución imaginable cuya IA está sometida por diseño a doble verificación humano-IA, transparencia por defecto y evidencia reproducible ante los tribunales (Caps. 8, 13). La estrategia se apoya en el mejor terreno en una generación: la confianza en la UE alcanzó en 2025 su máximo en 18 años (52%, ~60% entre los jóvenes de 15-24 años) precisamente mientras la confianza en las noticias caía a su mínimo histórico (37%, Reuters Institute 2026) y la preocupación por la desinformación subía del 28% (2022) al 36% (2025). El capítulo fija cuatro principios — **evidencia antes que opinión, transparencia por defecto, doble verificación también en comunicación, y aprender de los fracasos** (la Conferencia sobre el Futuro de Europa, las consultas públicas de objetivos poco claros que documentó el Tribunal de Cuentas) — y un instrumento emblemático: el **Informe Anual de Protección Cognitiva**, que publica hitos y resultados, nunca procedimientos ni técnicas. Cierra con el cronograma 2027-2040+ alineado con las fases del libro y con el horizonte del Capítulo 18: la comunicación que demuestra es la que convierte al PP en el referente que las democracias del mundo comprarán en 2049.

19.1 La tesis: hacer visible la protección

Toda institución nueva enfrenta dos batallas: existir y ser comprendida. El Poder Protector enfrenta una tercera que ninguna institución ha enfrentado antes: **ser creído en el ámbito exacto donde la creencia está rota**. Su función es proteger la esfera cognitiva — el territorio donde los ciudadanos han dejado de creer en lo que leen (confianza en las noticias: 37%, el mínimo desde 2015), donde desconfían de quien piensa distinto (7 de cada 10, Edelman 2026) y donde sospechan de toda máquina que decida sobre ellos (60% escépticos ante la IA gubernamental, OCDE 2026). En ese terreno, una estrategia de comunicación convencional — eslogan, campaña, hashtag — no solo fracasaría: **sería la prueba de lo que el crítico acusa** — otro actor más compitiendo por la atención con técnicas de persuasión.

Por eso la estrategia del PP es la contraria: **hacer visible la protección**. El PP no se define prometiendo lo que hará, sino mostrando lo que ya hizo y cualquiera puede comprobar: el informe forense con cadena de custodia, el expediente que la Comisión sancionó, el material manipulador expuesto con su método reproducible, el curso que el maestro de Bremen o de Lisboa puede descargar y usar. Cada acto de comunicación del PP debe ser **una demostración verificable, no una afirmación**. Y el objetivo es deliberadamente ambicioso, porque el momento lo permite: no se trata de que el ciudadano tolere al PP, sino de que **compre la idea** — que entienda que la protección cognitiva no es un control más, sino la condición de su libertad; que la Europa que la construye no es la Europa que regula tarde, sino la que produce el modelo de IA bajo control democrático que el mundo esperará en 2049. No es el momento de la falsa modestia: es el momento de que la evidencia hable — y de que la Unión se atreva a decir lo que la evidencia demuestra.

19.2 El terreno verificado: la paradoja del 60%

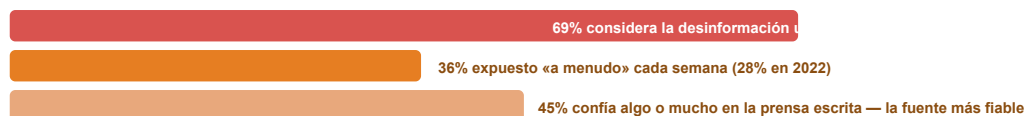
Los datos de 2025-2026 dibujan el terreno más difícil y el más favorable a la vez. El difícil: la confianza está rota en todos los frentes. La confianza en las noticias cayó al 37% — mínimo histórico desde que el Reuters Institute la

mide en 48 países (DNR 2026) — y el 42% de los ciudadanos evita las noticias, frente al 29% de 2017. La insularidad avanza: en el Edelman Trust Barometer 2026 (34.000 encuestados, 28 países), 7 de cada 10 dudan en confiar en quien tiene valores o fuentes de información distintos. Y el dato decisivo para este capítulo: el Trust Survey de la OCDE (jun-2026) muestra que **60% de los ciudadanos es escéptico ante el uso de la IA por sus gobiernos**. Los europeos exigen protección — el 69% considera un problema la desinformación en el Eurobarómetro de 2026 (85% en España, 82% en Chipre, 80% en Italia), y el 36% dice estar expuesto a ella "a menudo" o "muy a menudo" en la última semana (28% en 2022) — pero desconfían del instrumento que protegería. **Piden un escudo y sospechan del herrero.**

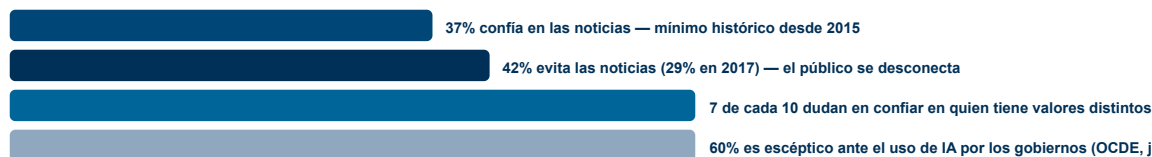
El terreno favorable: la Unión llega a esta batalla en su mejor momento de confianza en una generación. El Eurobarómetro de primavera 2025 registró la confianza en la UE en su **máximo en 18 años: 52%**, con cerca del 60% entre los jóvenes de 15-24 — la generación que consumirá toda su vida informativa en el terreno que el PP protege. Y la paradoja del 60% tiene una lectura estratégica que es el eje de este capítulo: **el escepticismo ante la IA gubernamental es universal y alcanzará también a los rivales** — el modelo autoritario no puede resolverlo porque su IA es por definición incontrolada por el ciudadano; el modelo del mercado no puede resolverlo porque su IA optimiza beneficios, no verificación. Solo el modelo del PP — IA sometida a doble verificación humano-IA, código abierto donde es posible, auditoría pública y evidencia reproducible — responde por diseño a la pregunta que el 60% se hace. **La paradoja del 60% no es el obstáculo del PP: es su argumento de venta más fuerte**, porque es el único en el mercado institucional cuya respuesta no es una promesa, es una arquitectura.

La paradoja del 60%: los europeos exigen protección y desconfían de la herramienta que la haría posible

LO QUE EXIGEN — preocupación y exposición (Eurobarómetro desinformación 2026; 26.500+ encuestados)



LO QUE SOSPECHAN — la confianza rota (Reuters DNR 2026 · Edelman 2026 · OCDE 2026)



LA PARADOJA: piden un escudo (69%) y sospechan del herrero (60%)

LA RESPUESTA DEL PP — la única arquitectura que responde por diseño a la pregunta del 60%

Doble verificación humano-IA (Cap. 8) · transparencia por defecto (Reg. 1049/2001) · evidencia reproducible ante los tribunales

Y la ventana: confianza en la UE en su máximo de 18 años (52%; ~60% entre los jóvenes de 15-24) — Eurobarómetro primavera 2025.

El modelo autoritario y el modelo del mercado no pueden resolver la paradoja del 60%: su IA no está bajo control ciudadano.

Figura 19.1 — La paradoja del 60% en datos verificados 2025-2026: la exigencia de protección, la confianza rota y la ventana de la UE — y por qué solo la arquitectura del PP la resuelve.

19.3 El marco de mensajes: comprar la idea

La tarea de la comunicación del PP es una transformación de percepciones — la misma que la Unión logró con el euro o con Erasmus: pasar de la abstracción técnica al derecho personal. El marco convierte cada objeción en su respuesta con evidencia del propio libro:

Percepción a transformar	Mensaje del Poder Protector	Evidencia que lo sostiene
«Es un gasto»	Es una inversión con retorno medible	ROI 164% a 5 años; +€1.820M/año de beneficio neto (Cap. 9B) — argumento adicional, nunca sustituto del cometido (Cap. 15)
«Es control»	Es libertad frente a la manipulación industrial	El PP no censura ni sanciona: detecta, audita, publica, remite y educa (Cap. 13) — el protector puro
«Es burocracia»	Es tecnología e innovación europea	Escáner forense, auditoría algorítmica y educación cognitiva en 24 lenguas sobre infraestructura propia (Cap. 18)
«Es restricción»	Es protección de derechos	La esfera cognitiva como derecho fundamental de la era digital (Caps. 1, 15)
«Es dependencia»	Es autonomía estratégica	Del 80% importado a la autonomía en tres fases, con Cláusula de Aceleración Estratégica (Cap. 18)
«Es otro regulador tardío»	Es el 4º poder: verificación antes que sanción	Base en el art. 48 TUE, recursos propios del art. 311 TFUE (Caps. 15, 16) — el poder que detecta nunca cobra lo que detecta
«¿Y su IA?» (la paradoja del 60%)	Nuestra IA es la única sometida a verificación pública permanente	Doble verificación humano-IA, herramientas abiertas, auditables y explicables (Caps. 8, 18) — la respuesta arquitectónica, no prometida

El mensaje central: el Poder Protector no es un freno, es el acelerador de la libertad europea — de la autonomía del ciudadano frente a la manipulación, del empleo cualificado del ecosistema (55.000-68.000 puestos, Cap. 17), y del liderazgo de la Unión como la democracia que hizo que la IA rindiera cuentas ante el ciudadano. Y la prueba no es el eslogan: es que cualquiera puede verificar cada afirmación del PP con la misma evidencia que un tribunal.

19.4 Los cuatro principios: demostrar, abrir, verificar, recordar

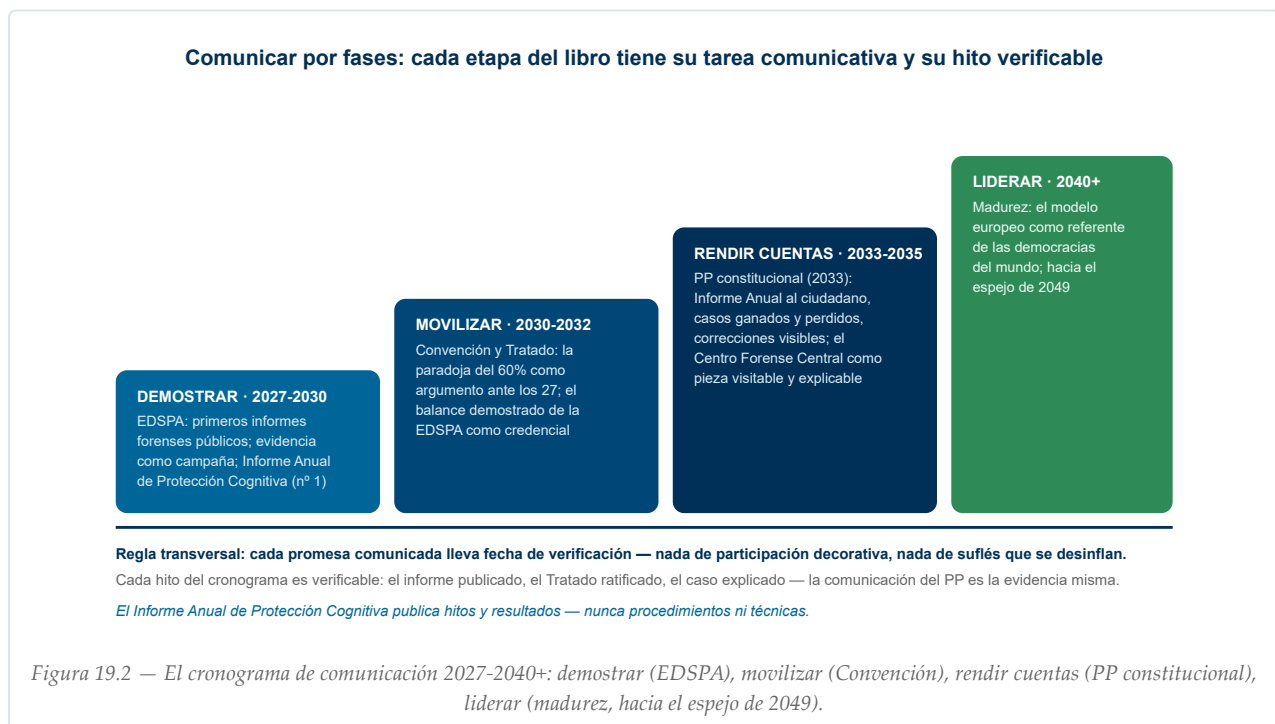
- Evidencia antes que opinión.** Cada comunicación relevante del PP va anclada a evidencia pública y reproducible: el informe forense, el expediente remitido, el dato auditado. El PP nunca pide que se le crea: muestra dónde está el expediente. En el terreno de la confianza rota (37%), la única moneda aceptada es la verificable.
- Transparencia por defecto.** El PP aplica a sí mismo el estándar que exige: derecho de acceso a documentos (art. 15(3) TFUE y Reglamento 1049/2001) como regla y no como excepción, publicación proactiva de sus criterios, decisiones e informes — incluido el resumen público sintético del radar «Estado de la Carrera Cognitiva» (Cap. 18). La regla de proporcionalidad que el libro fija en todo: **el PP publica hitos y resultados; nunca procedimientos ni técnicas** — la misma línea que separa el radar público del radar interno, porque la transparencia con el ciudadano no puede regalar la metodología al rival.
- Doble verificación también en comunicación.** Ninguna afirmación pública del PP sobre un caso, una cifra o un hallazgo se publica sin pasar por el mismo estándar que el PP exige a las plataformas: revisión humana de la salida de la máquina, trazabilidad de la fuente, corrección visible cuando se equivoca. La paradoja del 60% se cierra en cada acto comunicativo: el ciudadano ve, una y otra vez, que la IA del PP nunca habla sola.
- Aprender de los fracasos.** La Unión ya hizo el ejercicio contrario: la Conferencia sobre el Futuro de Europa (2021-2022) — 800 ciudadanos en paneles, 178 recomendaciones, 49 propuestas, 5 millones de visitas y 700.000 participantes — fue el ejercicio participativo más ambicioso jamás intentado, y su balance político quedó a medio camino; el Tribunal de Cuentas europeo documentó consultas públicas con objetivos poco claros y divulgación insuficiente; y la advertencia de la doctrina es antigua y certera: las consultas que no desembocan en nada desinflan el suflé y drenan la confianza. La lección para el PP es doble: **nada de participación decorativa** — cada mecanismo de escucha ciudadana del PP debe estar vinculado a una decisión con fecha y efecto visible — y nada de promesas sin seguimiento: el calendario que el PP publica, el PP cumple.

19.5 Los cinco públicos y el cronograma 2027-2040+

Los cinco públicos

- **Ciudadanos.** El mensaje: «sus decisiones, su esfera cognitiva, protegidas con evidencia que usted puede ver». La vía: el Informe Anual de Protección Cognitiva, los informes forenses públicos de casos emblemáticos, los materiales del Educador en 24 lenguas. El objetivo no es que el ciudadano conozca el Tratado: es que sepa *dónde mirar* cuando sospeche manipulación.
- **Formuladores de políticas.** El mensaje: viabilidad y ventana — base legal del art. 48 TUE, financiación por recursos propios (art. 311 TFUE, Cap. 16), ROI 164% (Cap. 9B), cronograma realista (PP constitucional 2033, Cap. 17). Y el argumento decisivo del capítulo: **la paradoja del 60% es imposible de responder con más regulación — solo con una institución de verificación permanente.**
- **Sector tecnológico europeo.** El mensaje: demanda institucional estable, procurement europeo y open source (la lección de Gaia-X, Cap. 18) — el PP como cliente ancla que convierte la capacidad europea en infraestructura de protección; el ecosistema de 55.000-68.000 empleos (Cap. 17) como prueba de que la protección cognitiva es un sector, no una carga.
- **Medios de comunicación.** El mensaje: el PP no compite con el periodismo — lo provee de evidencia verificable. Para una industria con confianza en mínimo histórico (37%), el PP es la fuente que ningún otro puede ofrecer: material forense reproducible, sin filtraciones interesadas. La regla: el PP trata a todos los medios con el mismo estándar de acceso — sin favoritos, sin exclusiones.
- **Comunidad internacional.** El mensaje: el modelo europeo de IA protectora de la esfera cognitiva como el referente de las democracias del mundo (Cap. 18) — el tercer camino entre el capitalismo algorítmico sin verificación y el control autoritario sin libertad, exportable como modelo institucional a toda democracia que enfrente la manipulación industrial.

El cronograma: demostrar, movilizar, rendir cuentas, liderar



El instrumento emblemático: el Informe Anual de Protección Cognitiva

Si el PP tuviera que resumir su comunicación en un solo acto, sería este: el **Informe Anual de Protección Cognitiva**, publicado cada año en las 24 lenguas de la Unión, presentado ante el Parlamento Europeo y abierto a cualquier ciudadano. Su contenido fija la regla de este capítulo: **hitos y resultados, nunca procedimientos ni técnicas** — qué amenazas se caracterizaron y con qué alcance, qué expedientes se remitieron y qué hicieron con ellos la Comisión y los Estados, qué materiales del Educador se usaron en las escuelas, dónde el PP falló y qué corrigió. Lo que el Informe no publica — método forense, capacidades del Escáner, arquitectura del radar — no es opacidad: es la misma línea de defensa que en el Capítulo 18, donde la transparencia rinde cuentas ante el ciudadano

sin regalar el mapa al rival. El Informe es, al mismo tiempo, el acto de rendición de cuentas más exigente que una institución europea haya publicado — y el mejor argumento de venta del PP: **un poder que enseña sus resultados, incluidos sus errores, es el único poder que el 60% escéptico puede empezar a creer.**

19.6 Conclusión: comunicar para liderar

1. **La comunicación del PP es función institucional, no marketing.** Un poder que protege la esfera cognitiva existe políticamente solo si el ciudadano puede verlo, verificarlo y entenderlo: hacer visible la protección es parte del cometido, no de la promoción.
2. **La paradoja del 60% es el eje y el argumento.** Los ciudadanos exigen protección frente a la desinformación (69%) y desconfían de la IA gubernamental (60%). Ningún modelo rival puede resolver esa contradicción; el PP la resuelve por arquitectura: doble verificación, transparencia por defecto, evidencia reproducible.
3. **El terreno es el mejor en una generación.** Confianza en la UE en máximo de 18 años (52%, ~60% en jóvenes) mientras la confianza informativa toca mínimos históricos (37%): la Unión llega a la batalla por la esfera cognitiva con autoridad creciente y un hueco exacto del tamaño del PP.
4. **Cuatro principios y una regla.** Evidencia antes que opinión, transparencia por defecto, doble verificación también en comunicación, aprender de los fracasos; y la regla de proporcionalidad: hitos y resultados, nunca procedimientos ni técnicas.
5. **Un instrumento y un cronograma.** El Informe Anual de Protección Cognitiva como acto de rendición de cuentas; demostrar (2027-2030), movilizar (2030-2032), rendir cuentas (2033-2035), liderar (2040+) — hacia el espejo de 2049 del Capítulo 18: la comunicación que demuestra es la que convierte al PP en el referente que las democracias del mundo comprarán.

La tesis del capítulo en una frase: en el terreno donde nadie cree a nadie, el único poder que puede ganar la batalla por la confianza es el que no pide que se le crea — el Poder Protector hace visible la protección: evidencia verificable, transparencia por defecto, IA que nunca habla sola, y la ambición de que la Europa que protege la esfera cognitiva de sus ciudadanos sea, en 2049, el modelo que el mundo democrático habrá comprado.

19.7 Fuentes y referencias verificadas

- **Percepción de la desinformación (Eurobarómetro, Comisión Europea):** Eurobarómetro sobre desinformación (edición 2025, 26.500+ encuestados): 36% expuesto «a menudo» o «muy a menudo» en los últimos 7 días (28% en el Eurobarómetro de 2022); Eurobarómetro publicado en feb-2026: 69% en la UE considera la desinformación un problema en su país (85% España, 82% Chipre, 80% Italia); 12% «muy seguro» y 52% «bastante seguro» de reconocer desinformación.
- **Confianza informativa:** Reuters Institute Digital News Report 2026 (casi 100.000 encuestados, 48 países, con la Universidad de Oxford): confianza en las noticias 37% — mínimo desde 2015; avoidance de noticias 42% (29% en 2017); las redes y plataformas de vídeo superan a la TV como fuente informativa global; interés por las noticias en descenso (-9 pp en Europa 2021-2026).
- **Confianza institucional y polarización:** Edelman Trust Barometer 2026 (34.000 encuestados, 28 países, trabajo de campo oct-nov 2025): el agravio deriva en insularidad — 7 de cada 10 poco o nada dispuestos a confiar en alguien con valores, planteamientos o fuentes de información distintos; reto global del arbitraje de la confianza.
- **Confianza en gobiernos y en la IA pública:** OECD Trust Survey 2026 (publicado 29-jun-2026): confianza en gobiernos nacionales ~40% en la OCDE; 60% de los encuestados escépticos ante el uso de la IA por instituciones gubernamentales (55% en Alemania); las experiencias positivas con servicios públicos fortalecen la confianza — la calidad de la administración importa más que la promesa política.
- **La ventana europea:** Eurobarómetro estándar primavera 2025: confianza en la UE 52% — máximo en 18 años; ~60% entre los jóvenes de 15-24 años; 75% se siente ciudadano de la UE; 62% optimista sobre el futuro de la Unión.
- **Participación y sus lecciones:** Conferencia sobre el Futuro de Europa (abr-2021 a may-2022): 800 ciudadanos en paneles deliberativos, 178 recomendaciones, 49 propuestas finales, 5 millones de visitantes de la plataforma, 700.000 participantes en eventos; balance de seguimiento calificado como «mixto» por el análisis académico (Carnegie Europe); Tribunal de Cuentas Europeo, informe especial 14/2019 sobre las consultas públicas de la

Comisión («Have your say!»): objetivos poco claros y divulgación insuficiente; doctrina de la comunicación europea: el riesgo del «suflé que se desinfla» — consultas sin resultados drenan confianza (Libaert/Euractiv); la propia Comisión asumió desde 2008 (Wallström) la necesidad de pasar «de la comunicación como venta a la participación».

- **Transparencia institucional:** art. 15(3) TFUE (derecho de acceso de todo ciudadano a los documentos de las instituciones) y Reglamento (CE) 1049/2001, de 30-may-2001, relativo al acceso del público a los documentos del Parlamento Europeo, del Consejo y de la Comisión.
- **Marcos propios del libro:** Cap. 8 (Escáner forense, doble verificación humano-IA), Cap. 9B (ROI 164%, + €1.820M/año), Cap. 13 (cinco verbos; protector puro), Cap. 15 (base legal art. 48 TUE; doctrina de la dotación), Cap. 16 (recursos propios art. 311 TFUE), Cap. 17 (PP constitucional 2033; ecosistema 55.000-68.000 empleos), Cap. 18 (autonomía en tres fases; radar con resumen público sintético; hitos y resultados, nunca procedimientos; referente 2049).

Capítulo 20: Camino Político y Legal del Poder Protector

La reforma del Tratado no es el obstáculo final: es la oportunidad histórica de convertir la protección de la esfera cognitiva en el proyecto fundacional de la Europa del siglo XXI — por un procedimiento que ya existe, ya fue activado por el Parlamento en 2023, y que el Poder Protector no tiene que inventar, solo que recorrer

Resumen del capítulo

Este capítulo responde a la pregunta que todo el libro deja pendiente: **¿cómo se aprueba políticamente un 4º poder constitucional en una Unión de 27 Estados que exige unanimidad?** La respuesta tiene tres niveles. Primero: **el camino legal ya existe y ya está desbrozado**. El procedimiento de revisión ordinaria del **art. 48(2-5) TUE** — Convención, Conferencia Intergubernamental, unanimidad, ratificación por todos según sus normas constitucionales — no es una hipótesis del libro: el Parlamento Europeo lo **activó formalmente el 22-nov-2023** con su informe de reforma de los Tratados (2022/2051(INL), 200+ páginas), el Consejo lo trasladó al Consejo Europeo el 18-dic-2023, y la presidenta von der Leyen apoyó públicamente la reforma en noviembre de 2024. La petición de Convención está sobre la mesa esperando a la coalición que la convoque; el Tratado del Poder Protector puede ser el texto que ella negocie. Segundo: **la estrategia es la coalición fundadora** — la cooperación reforzada como vía de arranque para los dispuestos (Cap. 14), sin cerrar la puerta a nadie, con la regla demostrada por la historia: no se obliga a un Estado a integrarse; se le demuestra que quedarse fuera es quedarse atrás. El precedente es verificable y reciente: **Dinamarca abolió su derogación de defensa por referéndum el 1-jun-2022 (~67% a favor; 66,9% exactos)**, tres décadas después de rechazarla, porque el contexto geopolítico cambió — igual que hará la evidencia de la EDSPA con los Estados reacios. Tercero: **la ventana geopolítica 2022-2026 es la mejor en una generación** — la ampliación con Ucrania obliga a reformar las instituciones antes de ensancharlas, la defensa europea demuestra que la Unión integra capacidades críticas cuando la amenaza lo exige, y los informes Draghi, Letta y Niinistö convergen en la misma conclusión: sin reforma estructural, no hay capacidad estratégica. El capítulo fija el procedimiento paso a paso, la cronología defendible del libro (firma 2031-2032, PP constitucional 2033), los riesgos y sus mitigaciones — y cierra con el espejo del Cap. 18: el rival tiene una estrategia con fecha (2049); este capítulo es la prueba de que las democracias también saben escribir la suya.

20.1 La tesis: el camino ya está desbrozado

El error de análisis más común sobre el Poder Protector es tratar la reforma del Tratado como el muro final del proyecto: unanimidad de 27, ratificación de 27, referéndums imposibles — y por tanto, nunca. Este capítulo demuestra lo contrario con un hecho verificable: **el procedimiento de reforma está formalmente activado desde 2023**. Tras la Conferencia sobre el Futuro de Europa (49 propuestas, varias de ellas exigiendo revisión de los Tratados), el Parlamento Europeo aprobó el 22-nov-2023 su informe sobre propuestas de modificación de los Tratados — un documento de más de 200 páginas de la comisión AFCO que propone reformas institucionales profundas — y ejerció el art. 48(2) TUE solicitando la convocatoria de una Convención. El Consejo lo trasladó al Consejo Europeo en diciembre de 2023. Desde entonces, la pelota está en el patio de los jefes de Estado y de Gobierno: la decisión de convocar la Convención se toma por **mayoría simple** (14 de 27 gobiernos) — no por unanimidad.

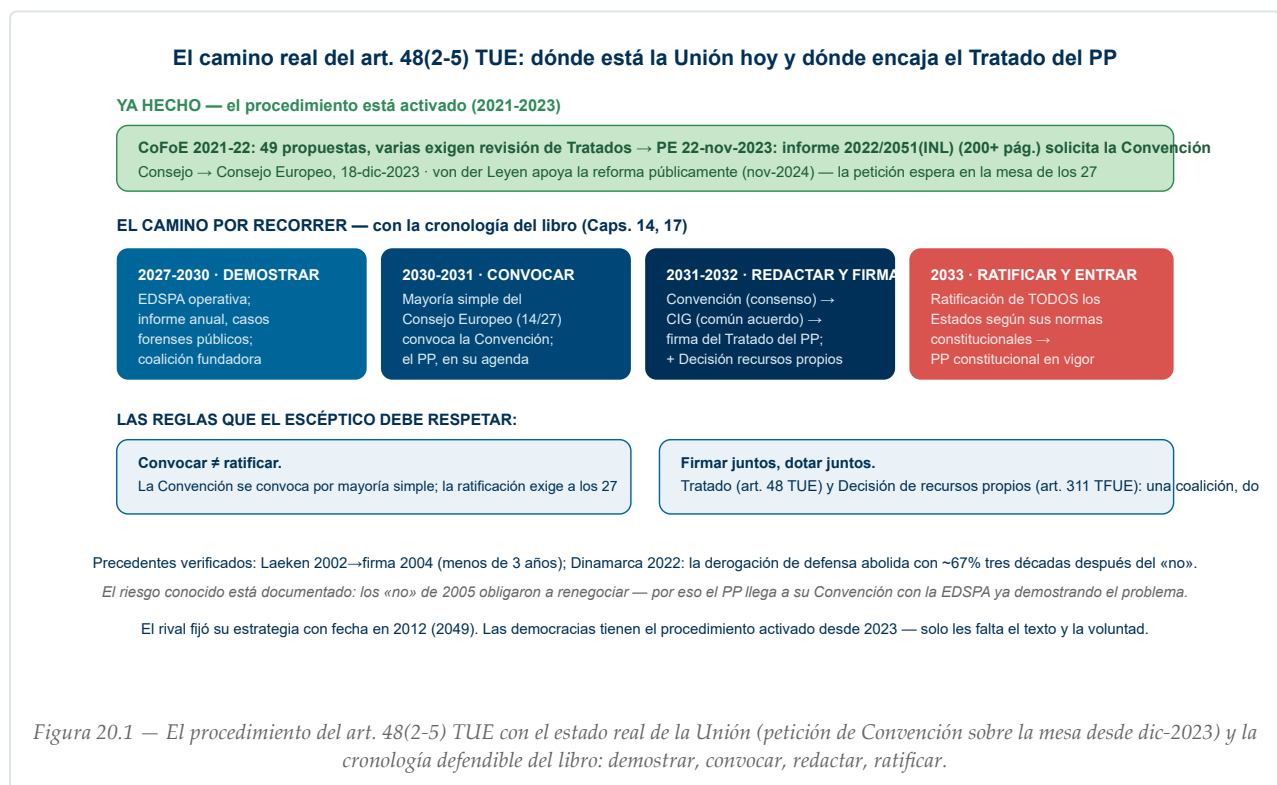
Esto cambia la naturaleza del problema del PP. No hay que convencer a 27 Estados de que inventen un procedimiento nuevo: hay que **colar el Tratado del 4º poder en una Convención que ya fue pedida, con el procedimiento ya escrito en el Tratado vigente y ya activado por la institución que lo hizo posible**. Y la tesis política del capítulo es deliberadamente ambiciosa: la reforma no es el coste del Poder Protector — es su **oportunidad histórica**. Cada paso del camino (la EDSPA que demuestra, la Convención que debate, la coalición que funda) no solo acerca el PP: obliga a la Unión a decidir, por primera vez con fecha y texto, qué modelo de esfera cognitiva quiere para el siglo XXI. El rival ya decidió el suyo en 2012 y le puso año: 2049. Este capítulo es el equivalente democrático de esa decisión.

20.2 El procedimiento real: art. 48(2-5) TUE paso a paso

El art. 48 TUE distingue dos vías. La **revisión ordinaria** (apartados 2-5) — la única que puede crear un nuevo poder constitucional — tiene cinco pasos:

1. **Propuesta.** La inicia un Estado miembro, el Parlamento Europeo o la Comisión ante el Consejo, que la traslada al Consejo Europeo. (Estado actual: hecha por el PE el 22-nov-2023; trasladada el 18-dic-2023.)
2. **Convención.** El Consejo Europeo decide **por mayoría simple** convocar una Convención — representantes de los parlamentos nacionales, de los jefes de Estado o de Gobierno, del Parlamento Europeo y de la Comisión — que examina las propuestas y adopta por consenso una recomendación. (Precedente: la Convención Laeken de 2002-2004, que redactó lo que sería el Tratado de Lisboa.)
3. **CIG.** La Conferencia Intergubernamental de representantes de los gobiernos aprueba las modificaciones **por común acuerdo**.
4. **Firma y entrada en vigor.** Las modificaciones entran en vigor **después de ser ratificadas por todos los Estados miembros conforme a sus respectivas normas constitucionales** — unanimidad real: ningún Estado queda fuera de la ratificación.
5. **Reforma electoral (si aplica).** El apartado 3 permite, para disposiciones de la parte tercera del TUE, un procedimiento simplificado sin Convención con aprobación unánime del Consejo Europeo — no aplicable al PP, que exige la vía ordinaria completa.

La cronología defendible del libro — ya fijada en los Capítulos 14 y 17 — cabe en este procedimiento con holgura histórica: **firma 2031-2032, ratificación completada y PP constitucional en 2033**. El precedente: de la Convención Laeken (feb-2002) a la firma del Tratado Constitucional (oct-2004) pasaron menos de tres años; y aunque los «no» francés y holandés de 2005 obligaron a la renegociación de Lisboa (2007, en vigor 2009) — la lección de esa crisis no es que la reforma sea imposible, sino que **el texto importa**: la Convención del PP llega con lo que a Laeken le faltó, una agencia que ya funciona y demuestra (EDSPA 2027-2030) el problema que el Tratado resuelve.



20.3 La estrategia: la coalición fundadora y el precedente danés

Ninguna estrategia de unanimidad empieza por la unanimidad. La del PP — ya fijada en el Capítulo 14 y financiada en el 16 — tiene tres piezas que este capítulo convierte en doctrina política:

Primera: no se obliga a integrarse; se demuestra que quedarse fuera es quedarse atrás. La cooperación reforzada (arts. 20 TUE y 326-334 TFUE) permite a los Estados dispuestos arrancar la EDSPA sin esperar al último — el mismo mecanismo con el que 25 Estados avanzaron la fiscalidad de transacciones financieras y el divorcio europeo. La puerta queda abierta; lo que no existe es el derecho a vetar a los demás. Y para el Estado que duda, la evidencia de la fase EDSPA (2027-2030) hará lo que hizo el contexto de 2022 con Dinamarca: **el 1 de junio de 2022, los daneses abolieron por referéndum su derogación de defensa con ~67% de los votos (66,9% exactos)** — una excepción que su país había defendido durante tres décadas (y reafirmado en 2000 y 2015) desapareció en un año, porque la agresión rusa cambió el cálculo de los votantes. Ningún tratado obligó a Copenhague: la realidad

lo hizo. La manipulación industrial hará lo mismo con cada Estado que vea a sus vecinos protegidos y sus propias elecciones expuestas.

Segunda: una coalición fundadora, dos actos juntos. El Tratado del PP (art. 48 TUE) y su Decisión de dotación (art. 311 TFUE) se tramitan con la misma geometría — unanimidad y ratificación nacional — y los mismos 27 firmantes potenciales. La coalición fundadora que los aprueba junta (Cap. 16) convierte dos batallas imposibles en una sola campaña: **un solo acto político dota al poder y lo financia.**

Tercera: la paradoja del 60% como argumento ante los gobiernos. El argumento decisivo ante un jefe de Estado escéptico no es el ROI (164%, Cap. 9B) ni el empleo (55.000-68.000, Cap. 17): es que **su propio electorado ya vive la contradicción** — exige protección frente a la desinformación (69% en la UE) y desconfía de la IA de su propio gobierno (60%, OCDE 2026) — y que ninguna cantidad de regulación reactiva resuelve esa contradicción, porque no es un problema legal: es institucional. Solo un poder de verificación permanente, con doble verificación humano-IA y transparencia por defecto, cierra el hueco que el 60% percibe. El gobernante que lo entienda no está aceptando una agencia más: está desactivando el argumento populista más potente de la próxima década — «ellos tienen la IA y tú no tienes nada que decir».

20.4 La ventana geopolítica 2022-2026: la mejor en una generación

Tres fuerzas convergen en la misma dirección, y ninguna la pidió este libro:

- **La ampliación obliga a la reforma.** Ucrania y Moldavia son candidatas; las negociaciones con Ucrania avanzan en nivel técnico pese al veto húngaro a la apertura formal (la presidencia danesa logró en nov-2025 el apoyo suficiente para el trabajo a nivel técnico). Ningún analista serio sostiene que la Unión puede absorber una ampliación de esa escala sin reformar sus instituciones y su toma de decisiones: la Convención pedida en 2023 es también la Convención de la ampliación — y el PP puede viajar en ella.
- **La defensa demostró que la Unión integra lo crítico.** El rearme tras 2022, la discusión abierta sobre un comisario de Defensa y una cláusula de defensa común, la dependencia del art. 42.7 TUE como garantía real para Kyiv: la Unión de 2026 ya está integrando la capacidad más celosamente soberana de todas, la militar, porque la amenaza lo exige. Si la defensa europea es hoy debatible, la protección de la esfera cognitiva — donde la amenaza ya opera contra todos los Estados miembros a diario — es constitucionalmente evidente.
- **Los informes de la propia Unión piden lo mismo.** Draghi (competitividad: fragmentación e incapacidad de escala), Letta (mercado único: huecos estructurales), Niinistö (preparación y resiliencia: amenazas híbridas y cognitivas) convergen en la misma conclusión con diferente vocabulario: **sin reforma estructural, la Unión no tendrá capacidad estratégica.** El PP es la traducción institucional de esa conclusión al ámbito donde la amenaza ya está dentro de casa.

Y sobre todo esto, el horizonte del Cap. 18: **el rival fijó su estrategia con fecha en 2012 — 2049.** No es una profecía de este libro; es un compromiso público del adversario con calendario y planes de ejecución verificables (China Standards 2035, autosuficiencia en semiconductores e IA como «proyecto nacional generacional»). La respuesta democrática no puede ser la regulación reactiva: tiene que ser una institución permanente con Tratado, dotación y fecha. La cronología de este capítulo — Convención hacia 2030, firma 2031-2032, PP constitucional 2033, pleno ~2037, madurez 2040+ — no es la velocidad máxima teórica: es **la velocidad mínima para que exista la segunda opción en 2049.**

20.5 La base legal como ventaja: lo que los Tratados ya dicen

La base del PP no es un artículo: es una **lectura coherente del derecho primario vigente** que este capítulo compacta (el desarrollo completo está en el Cap. 15):

Fundamento	Qué establece	Qué aporta al PP
Art. 2 TUE — valores de la Unión	Democracia, Estado de Derecho, derechos humanos como fundamento de toda la acción de la Unión	La esfera cognitiva es la condición material de esos valores: sin información verificable no hay democracia deliberativa posible
Art. 3 TUE — fines de la Unión	La Unión ofrece a sus ciudadanos un espacio de libertad, seguridad y justicia	La esfera cognitiva como espacio: la seguridad del ciudadano incluye la de su mente frente a la manipulación industrial
Art. 48(2-5) TUE — revisión ordinaria	Convención → CIG → ratificación de todos; activado por el PE en 2023	El procedimiento exacto para crear el 4º poder — ya pedido, ya desbrozado
Art. 16 TFUE + Carta arts. 7-8 — protección de datos	La protección de datos personales como derecho fundamental autónomo (con jurisprudencia del TJUE desde 2014: Google Spain)	El precedente constitucional de que el derecho protege activamente al ciudadano en su relación con la infraestructura digital
Art. 352 TFUE — cláusula de flexibilidad	Acción de la Unión cuando el Tratado no prevea los poderes necesarios para alcanzar sus fines (unanimidad)	La puerta legal de la EDSPA antes del Tratado: el medio no puede faltar cuando el fin es constitucional
Arts. 20 TUE + 326-334 TFUE — cooperación reforzada	Al menos 9 Estados pueden avanzar usando las instituciones de la Unión	La vía de arranque de la coalición fundadora: nadie veta a los dispuestos
Art. 311 TFUE — recursos propios	Dotación por Decisión unánime ratificada por todos	La financiación como categoría de la misma Decisión: un acto político dota y financia (Cap. 16)
Art. 222 TFUE — cláusula de solidaridad	La Unión y los Estados se prestan asistencia mutua ante un ataque (incluida la híbrida)	El marco donde las campañas de manipulación extranjeras son ya jurídicamente un ataque a un Estado miembro

Por qué esto es una ventaja y no un obstáculo: la Constitución del rival es un partido único que no necesita procedimientos. La de la Unión es un procedimiento que ya se ha ejecutado con éxito en cada ampliación institucional de su historia — de Laeken a Lisboa, del euro a los recursos propios de 2020. El PP no pide saltarse el derecho: pide usarlo por segunda vez en una generación para el fin que da sentido a todos los demás. La base legal no es el argumento de los escépticos — es el argumento del libro.

20.6 Conclusión: de la petición a la Convención

- 1. El camino existe y está activado.** Art. 48(2-5) TUE: Convención por mayoría simple, CIG por común acuerdo, ratificación de todos. El PE pidió la Convención en nov-2023; la petición espera al Consejo Europeo — el Tratado del PP puede ser su texto.
- 2. La estrategia es la coalición fundadora.** Cooperación reforzada para arrancar, puerta abierta para todos, y la regla demostrada por Dinamarca en 2022: los Estados no se obligan a integrarse — el contexto los convence, y la evidencia de la EDSPA hará de contexto.
- 3. El argumento ante cada gobierno es la paradoja del 60%.** Su electorado exige protección y desconfía de la IA estatal; solo una institución de verificación permanente con doble verificación y transparencia por defecto resuelve esa contradicción — y desactiva el populismo de la IA en vez de alimentarlo.
- 4. La ventana es real y verificada.** Ampliación con Ucrania que exige reformar antes de ensanchar, defensa europea integrando lo crítico, y Draghi/Letta/Niinistö convergiendo en la necesidad de reforma estructural: la Convención de 2030 tendrá que existir por razones que no son las del PP — el PP solo tiene que estar en ella.
- 5. Y la fecha de contrapeso es 2049.** El rival escribió su estrategia con centenario incluido; este capítulo demuestra que las democracias tienen el procedimiento, el precedente y la cronología (firma 2031-2032, PP 2033, pleno ~2037, madurez 2040+) para escribir la suya. Sin profecía — pero sin excusas.

La tesis del capítulo en una frase: la reforma del Tratado no es el muro final del Poder Protector: es la puerta que la Unión ya abrió en 2023 — y la oportunidad histórica de que la protección de la esfera cognitiva sea el proyecto fundacional de la Europa del siglo XXI, con el procedimiento del art. 48 TUE ya activado, la coalición fundadora ya definida y el espejo de 2049 ya encendido.

20.7 Fuentes y referencias verificadas

- **Derecho primario:** art. 48 TUE (revisión ordinaria: apartados 2-5; Convención convocada por mayoría simple del Consejo Europeo; CIG por común acuerdo; ratificación por todos los Estados según sus normas constitucionales; procedimiento simplificado del apartado 3 para la parte tercera del TUE, no aplicable al PP); arts. 20 TUE y 326-334 TFUE (cooperación reforzada: mínimo 9 Estados, uso de las instituciones); art. 352 TFUE (cláusula de flexibilidad); art. 311 TFUE (recursos propios); art. 222 TFUE (cláusula de solidaridad); art. 42.7 TUE (cláusula de asistencia mutua); art. 2 y 3 TUE (valores y fines); art. 16 TFUE y Carta de Derechos Fundamentales arts. 7, 8, 11 (privacidad, datos, información).
- **Estado real de la revisión (verificado):** Parlamento Europeo, resolución e informe 2022/2051(INL) «Propuestas del Parlamento Europeo de modificación de los Tratados», aprobados el 22-nov-2023 (comisión AFCD, 200+ páginas), activando el art. 48(2) TUE; el Consejo trasladó la petición al Consejo Europeo el 18-dic-2023; el Consejo Europeo no ha convocado aún la Convención; von der Leyen apoyó públicamente la reforma de los Tratados en nov-2024; análisis académico del proceso: West European Politics (2025) sobre los emprendedores de la revisión en el PE y las mayorías internas (aprobación del informe por 291 votos frente a 274, con divisiones en el PPE; la llamada previa a la Convención se había aprobado el 9-jun-2022 con 355:154:48).
- **Precedentes constitucionales:** Convención sobre el Futuro de Europa (Laeken, feb-2002 a jul-2003; informe final con proyecto de Tratado Constitucional, firmado oct-2004); «no» francés (may-2005) y holandés (jun-2005) en los referéndums de ratificación; Tratado de Lisboa (2007, en vigor 1-dic-2009); referéndums irlandeses sobre Lisboa: rechazo jun-2008, aprobación oct-2009 tras garantías.
- **El precedente danés:** referéndum del 1-jun-2022: abolición de la derogación danesa en materia de defensa con ~67% de los votos (anunciado en mar-2022 tras acuerdo interpartidario), tres décadas después de las derogaciones de Edimburgo (1992) y de los referéndums de 2000 (euro, rechazado) y 2015 (conversión de la derogación de justicia e interior, rechazada); el contexto: la agresión rusa contra Ucrania.
- **Ampliación y defensa (contexto 2025-2026):** Ucrania y Moldavia candidatas (2022); el veto húngaro a la apertura formal de negociaciones de adhesión con Ucrania y el trabajo técnico continuado bajo la presidencia danesa (nov-2025); el art. 42.7 TUE como garantía discutida en las conversaciones de seguridad para Ucrania; debate europeo sobre un comisario de Defensa y una cláusula de defensa común en el marco de la respuesta al rearme.
- **Informes de la Unión:** Informe Draghi (2024) sobre competitividad; Informe Letta (2024) sobre el mercado único «Mucho más que un mercado»; Informe Niinistö (2024) sobre preparación ante crisis y amenazas (incluidas las híbridas y de desinformación); Conference on the Future of Europe, informe final (may-2022): 49 propuestas, incluida la revisión de los Tratados.
- **Marcos propios del libro:** Cap. 9B (ROI 164%), Cap. 14 (doble vía constitucional: EDSPA por cooperación reforzada → Tratado), Cap. 15 (base legal desarrollada; art. 352 TFUE y jurisprudencia TJUE), Cap. 16 (un acto político dota y financia: art. 48 TUE + art. 311 TFUE), Cap. 17 (cronología: firma 2031-2032, PP constitucional 2033; ecosistema 55.000-68.000), Cap. 19 (paradoja del 60% como argumento ante los gobiernos), Cap. 18 (espejo 2049: Dos Centenarios, China Standards 2035).

Capítulo 21: El futuro no se predice: se construye

El futuro no se predice: se construye. Y Europa ya sabe construir: exportó paz donde hubo mil años de guerras, protegió la privacidad del europeo y terminó protegiendo la del mundo, creó una identidad con becas de estudio. El Poder Protector sería la cuarta vez que Europa hace lo que nadie más puede hacer — y la condición para que la inteligencia artificial sea el próximo salto del ser humano y no su sustituto

Resumen del capítulo

Este capítulo cierra el libro. No con una profecía sino con algo más difícil y más honesto: **una visión construida sobre lo que ya existe y lo que Europa ya ha demostrado saber hacer**. Primero, los **tres modelos digitales en competencia** (mercado, control, democracia) son un hecho de 2026, no del futuro; este capítulo los compara sin veredictos y muestra lo que cada uno *no puede dar por diseño* — el mercado no puede monetizar la atención y protegerla a la vez; el control no puede separar la protección de la vigilancia; solo el modelo europeo puede combinar las dos cosas, y solo si tiene un ejecutor permanente: el hueco institucional que este libro demuestra. Segundo, **el mundo ya pide lo que Europa puede dar**: los Principios Globales de la ONU para la Integridad de la Información (Guterres, jun-2024), el primer tratado mundial vinculante sobre IA y derechos humanos del Consejo de Europa (abierto a firma sep-2024, firmado por la Comisión en nombre de la UE) y los Principios OCDE de IA actualizados en 2024 — la doctrina global existe; falta la institución que la encarnice de forma permanente y verificable. Tercero, **el legado no se mide en cifras mágicas sino en lo ganado por diseño**: una institución duradera con recursos propios, el juicio humano institucionalizado como contrapeso de la IA, una sociedad alfabetizada y Europa como referente de las democracias del mundo. Y cuarto, el cierre que el libro merece: **la elección de 2049, el sueño declarado como sueño** — el precedente de Gutenberg: la imprenta también ahogó al hombre en palabras ajenas, y de esa explosión nacieron el humanismo y la educación; la IA es la imprenta del siglo XXI, y Europa puede inventar su humanismo digital — y el llamado a la acción: este libro no es un análisis, es una llamada. El momento es ahora.

21.1 La tesis: el futuro no se predice, se construye

Una frase resume la tentación: «quien controla la esfera digital controla el mundo. Y en 2039, Europa lo hará». Este libro ha trabajado durante veinte capítulos para demostrar lo contrario de esa frase — que **nadie controla la esfera digital**, y que la ambición europea no es controlarla sino **proteger a quien la habita**. Y también para demostrar que las profecías son el método de los rivales: el Dos Centenarios de Xi Jinping y China Standards 2035 son precisamente eso, profecías con fecha. Las democracias no profetizan: **construyen**.

La tesis de este cierre es que el futuro del Poder Protector no es una predicción sino **una decisión**. Cada elemento ya existe y ha sido verificado en este libro: el **acervo normativo** (AI Act, DSA, DMA, Escudo Europeo de la Democracia, Paquete de Soberanía — Cap. 13); el **procedimiento** de reforma ya activado por el Parlamento Europeo (art. 48 TUE, Cap. 20); la **vía de arranque** para los dispuestos (cooperación reforzada, Cap. 14); la **financiación autónoma** (recursos propios, art. 311 TFUE, Cap. 16); la **tecnología por fases** con cláusula de aceleración (Cap. 18); la **evidencia económica** (ROI 164%, +€1.820M/año, Cap. 9B) y la **estrategia de comunicación** que resuelve la paradoja del 60% (Cap. 19). Nada de esto depende de adivinar el futuro. Depende de que treinta y años de decisión política europea se alineen — como se alinearon, durante décadas, para construir la paz.

De víctima a arquitecto: esa es la transformación que este libro ha ido montando pieza a pieza. La víctima sufre la esfera cognitiva; el arquitecto la diseña. Entre una y otra cosa hay exactamente una institución: el Poder Protector.

21.2 Tres modelos en competencia: lo que cada uno puede — y lo que no puede dar

El mundo digital de 2026 no tiene un dueño: tiene **tres modelos en competencia**, cada uno con un principio organizador distinto. No son hipótesis: conviven, compiten y exportan sus lógicas hoy.

Modelo	Representante	Principio	Fortalezas verificadas	Debilidades verificadas
Capitalismo digital	EE.UU.	Innovación privada + mercado	Ecosistema emprendedor sin igual; liderazgo en modelos fundacionales y semiconductores; velocidad de despliegue	Su motor es la economía de la atención: el tiempo del ciudadano es la materia prima que se monetiza; la regulación de su esfera digital la impone un tercero (DSA/DMA europeos); crisis de confianza informativa global (Edelman 2026: 7/10 ciudadanos en cámaras de eco)
Autoritarismo digital	China	Control estatal + escala	Estrategia a décadas vista y publicada (Dos Centenarios, China Standards 2035); autosuficiencia acelerada (Kirin 7nm sin EUV, Ascend 910C/950 con memoria propia; subsidios ~\$150.000M; autosuficiencia 16%→28% en 18 meses)	Censura y vigilancia masiva por diseño; la misma infraestructura que protege del exterior vigila al interior; exporta control (Ruta de la Seda Digital), no protección
Democracia digital	Europa	Innovación + derechos + ley	El único acervo normativo digital completo del mundo (AI Act, DSA, DMA, RGPD, Escudo Europeo de la Democracia); confianza ciudadana en la UE en máximo de 18 años (52%); el modelo que otros copian (efecto Bruselas)	80% de la infraestructura digital importada (EuroStack/Bertelsmann 2025); el consenso de 27 es lento; sin ejecutor permanente, la ley protege en el papel

La tabla no declara un ganador — no lo hay todavía, y este libro no profetiza. Pero sí permite ver algo que las tres columnas esconden:

Lo que cada modelo no puede dar — por diseño, no por casualidad

El mercado no puede proteger la esfera que monetiza. No es una acusación moral: es una estructura de incentivos. Cada mejora en la protección de la atención del ciudadano es, para el modelo que vive de ella, un coste. Por eso la única regulación seria de la esfera digital estadounidense la escribió otro: Europa.

El control no puede dar libertad. El aparato técnico que detecta manipulación externa es el mismo que vigila al disidente interno; comparten infraestructura, derecho público y personal. Por diseño, proteger conlleva vigilar. Por eso exporta censura, no protección.

La democracia europea puede las dos cosas — pero solo con ejecutor. El acervo normativo ya define protección *con* libertad. Lo que no tiene es la institución permanente e independiente que lo haga verdad cada día. Y solo el modelo europeo resuelve la paradoja del 60% (69% de los europeos exige protección frente a la desinformación; 60% desconfía de la IA gubernamental): la doble verificación humano-IA, la transparencia por defecto y la evidencia reproducible convierten la desconfianza en condición de diseño del poder, no en su riesgo. Los otros dos modelos no pueden resolver esa paradoja: el mercado no puede responder a quien desconfía de su incentivo, y el control no puede responder a quien teme su vigilancia.

La diferencia decisiva: las debilidades del mercado y del control son estructurales — no se corrigen sin dejar de ser lo que son. La debilidad europea es de ejecución, y la ejecución se corrige dentro del propio modelo: es exactamente el contenido de los Capítulos 14 a 20 de este libro.

21.3 El mundo ya pide lo que Europa puede dar

Europa no necesita imaginar un mundo que espere su tecnología: la realidad verificada de 2024 es mejor: **el mundo ya pidió — formalmente, por escrito — lo que Europa puede dar.** Tres documentos, tres instituciones globales:

- **Las Naciones Unidas: Principios Globales para la Integridad de la Información** (Guterres, 24-jun-2024). El Secretario General pidió «responder a los daños causados por la difusión del odio y las mentiras en línea

defendiendo vigorosamente los derechos humanos» y advirtió que las amenazas a la integridad de la información «se proliferan y expanden con velocidad sin precedentes, potenciadas por la IA». Los Principios — surgidos de su informe *Nuestra Agenda Común* (2021) — exigen un ecosistema informativo más humano y sirvieron de base para la Cumbre del Futuro (sep-2024). Es la doctrina global: falta el ejecutor.

- **El Consejo de Europa: Convenio Marco sobre Inteligencia Artificial y Derechos Humanos, Democracia y Estado de Derecho** — el primer tratado internacional jurídicamente vinculante del mundo sobre IA, abierto a firma el 5-sep-2024 en Vilna. La Comisión Europea lo firmó en nombre de la Unión. Un tratado vinculante que compromete a sus partes a que los sistemas de IA no socaven la integridad democrática: la comunidad jurídica de las democracias ya lo escribió. Falta la institución que lo verifique todos los días.
- **La OCDE: Principios sobre IA** — el primer estándar intergubernamental de IA (2019), actualizado en el Consejo Ministerial de may-2024 para la era de la IA generativa: cinco principios basados en valores y cinco recomendaciones para gobiernos. El lenguaje común de las democracias sobre IA que respeta derechos.

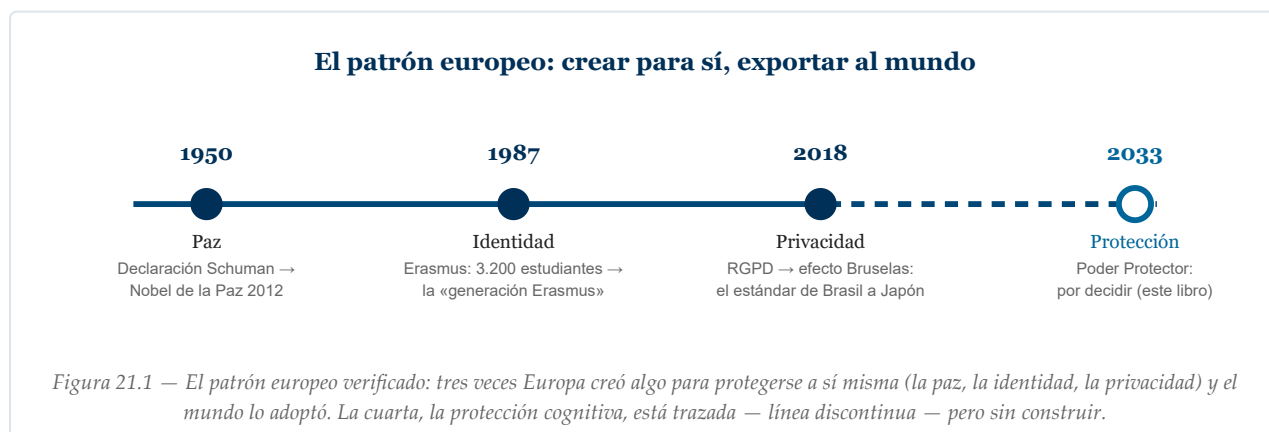
Y en casa, el marco oficial donde la misión encaja sin forzar nada: el **Programa del Decenio Digital 2030** (Decisión (UE) 2022/2481) fija como objetivos de la Unión **20 millones de especialistas TIC empleados, el 80% de los adultos de 16 a 74 años con competencias digitales básicas y el 75% de las empresas usando cloud/IA para 2030**. El Poder Protector no llega a un continente sin plan: llega a un continente con metas oficiales de alfabetización y capacidades digitales que su función educativa (Cap. 12: alfabetización $\geq 90\%$ en 2038) sirve directamente, y con una doctrina global ya escrita que su función ejecutiva encarna.

El patrón tiene precedente verificado: el **efecto Bruselas**. El RGPD, nacido en 2018 para proteger al europeo, se convirtió en modelo de legislación en Brasil, Japón, Singapur, Sudáfrica, Corea del Sur, Sri Lanka, Tailandia y decenas más de jurisdicciones. Europa reguló para sí y terminó escribiendo el estándar mundial de privacidad sin disparar un solo misil normativo. Si el Poder Protector madura, la misma mecánica puede operar con la protección cognitiva: las democracias del mundo no necesitan copiar una agencia europea — necesitan el *modelo*: un poder constitucional, independiente, con verificación doble y evidencia pública. Nadie más lo tiene. Nadie más lo está construyendo.

21.4 El legado: lo que habrá cambiado — recapitulación y lo ganado por diseño

El camino recorrido en este libro, en cuatro partes:

- **Parte I — El problema (Capítulos 1-5):** la esfera cognitiva digital como bien público esencial capturado: manipulación industrial, interferencia electoral, dependencia tecnológica. El diagnóstico: Europa era víctima en su propia esfera.
- **Parte II — El parche (Capítulos 6-10, con 9 y 9B):** la EDSPA: una agencia especializada que protege ya — verificable en su economía (ROI 164%, +€1.820M/año) — y que existe, ante todo, para demostrar que la protección cognitiva funciona antes de pedirle a 27 Estados que la constitutionalicen.
- **Parte III — La Solución Definitiva (Capítulos 11-20):** de la agencia al poder: arquitectura institucional, competencias de protector puro, transición sin vacío, base legal, recursos propios, impacto económico, tecnología por fases, comunicación que resuelve la paradoja del 60% y el procedimiento político ya activado desde 2023.
- **Parte IV — La visión (este capítulo):** no una predicción, sino la declaración de lo que Europa puede ser si decide serlo.



¿Y el legado del Poder Protector? No una tabla de cifras mágicas. El legado real se mide en lo que la arquitectura garantiza **por diseño**, y en las cifras que este libro sí verificó:

- **Una institución que dura.** Un poder constitucional con recursos propios (art. 311 TFUE) no depende del ciclo electoral ni del presupuesto anual: es la primera garantía de que la protección de la esfera cognitiva deja de ser una moda política y se vuelve infraestructura de la democracia — como lo son hoy el banco central o la justicia.
- **El juicio humano como empleo institucional.** La trayectoria de dotación verificada en el libro — de 1.500-2.000 (EDSPA) a más de 15.000 empleados en madurez 2040+ (Caps. 15-16), con 55.000-68.000 empleos en el ecosistema (Cap. 17) — no es un plan de empleo: es el contrapeso de la IA. El Poder Protector sería el mayor empleador público europeo del juicio humano no automatizable: en la era de la automatización del pensamiento, mantener a miles de personas dedicadas profesionalmente a verificar con criterio es una política civilizatoria, no una nómina.
- **Una sociedad alfabetizada.** La función educativa del PP (Cap. 12) sirve directamente las metas oficiales del Decenio Digital (80% de competencias básicas, 20 millones de especialistas TIC para 2030) y las extiende a la alfabetización cognitiva: el ciudadano que reconoce la manipulación es la última línea de defensa — la única que ningún adversario puede hackear.
- **Europa como referente de las democracias.** Si el modelo madura, las democracias del mundo que hoy no tienen respuesta propia a la manipulación industrial tendrán un modelo que copiar — verificable, constitucional, compatible con la libertad. Sin profecía de victoria: como la privacidad se globalizó sin que nadie la «ganara», la protección puede expandirse porque funciona y se copia, no porque Europa la imponga.
- **La evidencia como bien común.** El Informe Anual de Protección Cognitiva (Cap. 19), la base de evidencia forense pública y la doctrina del «hitos y resultados, nunca procedimientos» dejan algo que hoy no existe en el mundo: un archivo público y verificable de cómo se manipula a las democracias y cómo se resiste — un bien público global que ningún otro modelo producirá nunca, porque el mercado no puede y el control no querrá.

21.5 El cierre: dos modelos terminados, un sueño declarado y una llamada

La elección de 2049

En 2049, la República Popular China celebra su centenario con un objetivo público y declarado: ser la potencia tecnológica total. Su modelo estará terminado: control estatal de la información, vigilancia interior exportada como infraestructura, estándares propios. Estados Unidos también tendrá el suyo: la esfera cognitiva como mercado, con su crown jewels en algoritmos y chips. El mundo que hoy nace digital tendrá que elegir entre los dos — **a menos que exista un tercero**: el que combine tecnología de vanguardia, libertad y protección verificada. Ese tercero no existirá por generación espontánea. Este libro es el plano para construirlo a tiempo.

No es una profecía de victoria — es una ventana de relevancia. La paradoja de las democracias es que casi siempre llegan tarde pero casi nunca llegan equivocadas: llegaron tarde a la revolución industrial y la terminaron liderando, tarde al bienestar y lo defendieron, tarde a la privacidad digital y hoy escriben su estándar. Llegarán tarde a la protección cognitiva. Que no lleguen tarde para siempre: de eso va este libro.

El sueño: por qué Europa puede permitirse soñar

Lo que sigue es una aspiración declarada — no una predicción.

Cuando Gutenberg imprimió, Europa se ahogó en palabras. La imprenta multiplicó la información — y con ella la manipulación: profecías impresas, panfletos de guerra, indulgencias vendidas a escala industrial. Durante un siglo, la explosión informativa parecía el apocalipsis. Y de esa misma explosión nacieron el humanismo renacentista, la Reforma, la educación universal y, al final del camino, la libertad de pensamiento como derecho. **Europa no respondió a la imprenta prohibiéndola: respondió educándose.** La respuesta a la manipulación por la palabra impresa no fue menos imprenta: fue más humanismo.

La inteligencia artificial es la imprenta del siglo XXI: multiplica la información y con ella la manipulación — deepfakes, bots, narrativas industriales. La tentación de prohibir es la vieja tentación; la respuesta europea histórica es la otra: **el humanismo digital**. Y Europa inventó el humanismo una vez, cuando la información se multiplicó y el hombre parecía ahogarse en palabras ajenas; puede inventar su versión digital: el ser humano libre de manipulación, usando la inteligencia artificial como usó la imprenta — para pensar más y mejor.

Y si la ambición parece grande, que sea el precedente el que la sostenga. **Europa ya lo ha hecho tres veces.** Schuman, en 1950, soñó la paz imposible — «la paz mundial no puede salvaguardarse sin esfuerzos creativos propor-

cionales a los peligros que la amenazan» — y de esa frase nació la reconciliación donde hubo mil años de guerras; el Nobel de la Paz de 2012 lo certificó: seis décadas de paz, reconciliación, democracia y derechos humanos. El RGPD, en 2018, protegía al europeo — y terminó protegiendo la privacidad de Brasil a Japón, de Sudáfrica a Corea del Sur, sin que nadie lo pidiera: el mundo lo copió porque funcionaba. Erasmus, en 1987, empezó con 3.200 estudiantes de 11 países — y creó algo que no existía: una generación europea. **El Poder Protector sería la cuarta vez que Europa crea para sí lo que el mundo estaba esperando.** Ningún otro continente tiene ese patrón. Ningún otro puede permitirse este sueño.

La llamada

Este libro empezó con una esfera capturada y termina con un plano completo: el diagnóstico, el parche que demuestra, el camino jurídico y financiero ya verificado, y la visión. Hay una frase que no necesita corrección ninguna: **este libro no es solo un análisis, es una llamada a la acción.** El futuro de Europa — y de toda democracia que quiera sobrevivir digital sin dejar de ser libre — depende de que tomemos hoy la decisión de proteger la esfera cognitiva. El Poder Protector es el vehículo. El momento es ahora.

Una generación protegida de la manipulación puede usar la inteligencia artificial para el siguiente salto humano: pensar más y mejor. A eso aspira Europa. A eso aspira este libro.

21.6 Fuentes y referencias verificadas

- **Marco global verificado:** Naciones Unidas, Principios Globales para la Integridad de la Información, lanzados por el Secretario General António Guterres el 24-jun-2024 (origen: *Nuestra Agenda Común*, 2021; base para la Cumbre del Futuro, sep-2024). Consejo de Europa, Convenio Marco sobre Inteligencia Artificial y Derechos Humanos, Democracia y Estado de Derecho: primer tratado internacional jurídicamente vinculante sobre IA, abierto a firma el 5-sep-2024 (Vilna); firmado por la Comisión Europea en nombre de la UE. OCDE, Principios sobre IA: primer estándar intergubernamental de IA (2019), revisado por el Consejo Ministerial de may-2024 (cinco principios de valores, cinco recomendaciones).
- **Marco europeo oficial:** Programa del Decenio Digital (Decisión (UE) 2022/2481): objetivos 2030 de 20 millones de especialistas TIC empleados, 80% de adultos de 16-74 años con competencias digitales básicas, 75% de empresas usando cloud/IA; informe *State of the Digital Decade* de la Comisión.
- **Precedentes del patrón europeo:** Declaración Schuman (9-may-1950): «la paz mundial no puede salvaguardarse sin esfuerzos creativos proporcionales a los peligros que la amenazan»; Premio Nobel de la Paz 2012 a la UE «por más de seis décadas de contribución al avance de la paz, la reconciliación, la democracia y los derechos humanos en Europa»; RGPD (2018) y efecto Bruselas: modelo de legislación en Brasil, Japón, Singapur, Sudáfrica, Corea del Sur, Sri Lanka, Tailandia y otras jurisdicciones; Erasmus (1987): 3.200 estudiantes de 11 países en su primer año; la «generación Erasmus» como identidad.
- **Contexto rival (verificado, Cap. 18):** Dos Centenarios de Xi Jinping (anunciados en el XVIII Congreso, 2012: sociedad moderadamente próspera para el centenario del Partido Comunista, 2021; país plenamente modernizado para el centenario de la República Popular, 2049, con hito intermedio de «modernización socialista básica» en 2035), China Standards 2035, autosuficiencia semiconductora acelerada (Kirin 7nm sin EUV, Ascend 910C/950, subsidios ~\$150.000M, 16%→28% en 18 meses, metas declaradas: 70% del plan Made in China 2025 (no alcanzada) y 80% para 2030).
- **Tres modelos 2026 (verificados):** economía de la atención como modelo de negocio; Edelman 2026 (34.000 encuestados, 28 países; insularidad informativa 7/10); DSA/DMA europeos regulando la esfera digital de las plataformas; Ruta de la Seda Digital; EuroStack/Bertelsmann 2025 (80% de infraestructura importada); Eurobarómetro primavera 2025 (confianza UE 52%, máximo 18 años).
- **Marcos propios del libro:** Cap. 9B (ROI 164%, +€1.820M/año), Cap. 12 (alfabetización ≥90% en 2038; trayectoria de dotación), Caps. 15-16 (recursos propios, art. 311 TFUE; >15.000 empleados en madurez 2040+), Cap. 17 (ecosistema 55.000-68.000 empleos), Cap. 19 (paradoja del 60%; Informe Anual de Protección Cognitiva; hitos y resultados, nunca procedimientos), Cap. 18 (espejo 2049; cláusula de aceleración), Cap. 20 (art. 48 TUE activado 22-nov-2023).

Nota de rigor sobre la visión: las secciones 21.4 y 21.5 contienen aspiraciones declaradas («el sueño», la frase final) deliberadamente marcadas como tales — ninguna es predicción ni dato. Las únicas cifras del capítulo son las verificadas en el libro (ROI 164%, +€1.820M/año, 55.000-68.000 empleos, >15.000 empleados 2040+, 80% infraestructura importada) y las fuentes de la sección 21.6. El centenario de la RPC es 2049.

Anexo A: Textos Legales

Propósito del anexo

Este anexo reúne los **textos jurídicos reales** en los que se apoya la propuesta del libro, citados literalmente y con su referencia oficial. La regla es estricta: **nada de lo que aparece aquí es un documento inventado** — cada cita corresponde a las versiones consolidadas de los Tratados (DOUE C 326, 26-10-2012), a reglamentos con número y fecha oficiales, a jurisprudencia del TJUE con número de asunto, o a actos y paquetes verificables de las instituciones. El anexo se organiza en tres bloques: la base de la EDSPA (sin reforma del Tratado), la base del Poder Protector (con reforma) y el acervo que ambas instituciones harán ejecutivo.

A.1 Base jurídica de la EDSPA (2027-2030): sin reforma del Tratado

Artículo 114 TFUE — Aproximación de legislaciones (mercado interior)

«El Parlamento Europeo y el Consejo, con arreglo al procedimiento legislativo ordinario y previa consulta al Comité Económico y Social, adoptarán las medidas relativas a la aproximación de las disposiciones legales, reglamentarias y administrativas de los Estados miembros que tengan por objeto el establecimiento y funcionamiento del mercado interior.»

TFUE, art. 114, apartado 1 (DOUE C 326, 26-10-2012)

Aplicación a la EDSPA: la fragmentación de la protección cognitiva entre Estados miembros distorsiona el mercado interior digital; la aproximación de disposiciones mediante reglamento es la vía ordinaria por la que la Unión ha creado todos sus marcos digitales. Es la base principal del reglamento EDSPA, en línea con la doctrina del Cap. 15 (jerarquía de bases: reglamento primero).

Artículo 16 TFUE — Protección de datos personales

«Toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan.»

TFUE, art. 16, apartado 1 (DOUE C 326, 26-10-2012)

Aplicación a la EDSPA: la esfera cognitiva se compone, en gran medida, de datos personales tratados a escala industrial; el art. 16 es la base constitucional del RGPD y el ancla de toda la legislación de protección que la EDSPA audita. Complementado por los arts. 7 y 8 de la Carta (sección A.2).

Artículo 352 TFUE — Cláusula de flexibilidad

«Si una acción de la Unión resultase necesaria, en el marco de las políticas definidas en los Tratados, para alcanzar uno de los objetivos fijados por los mismos, sin que los Tratados hayan previsto los poderes de actuación necesarios a tal efecto, el Consejo, por unanimidad, a propuesta de la Comisión y previa aprobación del Parlamento Europeo, adoptará las disposiciones pertinentes.»

TFUE, art. 352, apartado 1 (DOUE C 326, 26-10-2012)

Aplicación a la EDSPA: base subsidiaria: si el legislador considerase insuficiente el art. 114, el 352 permite adoptar la acción necesaria para un objetivo del Tratado (la protección de un espacio de libertad, seguridad y justicia, o el mercado interior). Requiere unanimidad, por lo que su valor aquí es de respaldo doctrinal, no de vía principal.

Cooperación reforzada: artículo 20 TUE y artículos 326-334 TFUE

«Los Estados miembros que deseen establecer entre sí una cooperación reforzada en el ámbito de las competencias no exclusivas de la Unión podrán utilizar a tal efecto las instituciones de la Unión y ejercer dichas competencias aplicando las disposiciones pertinentes de los Tratados. [...] La cooperación reforzada sólo podrá ser autorizada por el Consejo como último recurso, cuando quede constatado que los objetivos perseguidos por dicha cooperación no pueden ser alcanzados en un plazo razonable por la Unión en su conjunto [...] La cooperación reforzada estará abierta en todo momento a los demás Estados miembros, con arreglo al artículo 331 del Tratado de Funcionamiento de la Unión Europea.»

TUE, art. 20, apartados 1 y 2 (DOUE C 326, 26-10-2012)

«La cooperación reforzada tendrá por objeto impulsar la realización de los objetivos de la Unión, proteger sus intereses y reforzar su proceso de integración. [...] Los actos y decisiones adoptados en el marco de una cooperación reforzada no vincularán sino a los Estados miembros participantes.»

TFUE, art. 326, apartados 1 y 2 (DOUE C 326, 26-10-2012)

Aplicación a la EDSPA (coherente con los Capítulos 11 y 14):

- **Mínimo de 9 Estados miembros** para constituir la (art. 20 TUE) — el núcleo fundador del libro.
- **Último recurso:** la autorización exige constatar que la Unión en su conjunto no puede alcanzar el objetivo en plazo razonable — precisamente el diagnóstico de la Parte I (la Unión en su conjunto no ha protegido la esfera cognitiva).
- **Apertura permanente (art. 331 TFUE):** cualquier Estado miembro puede notificar su intención de sumarse; la Comisión confirma su participación en el plazo de cuatro meses. La unión gradual modelo Schengen del Cap. 14 tiene su mecánica literal aquí.
- Los actos solo vinculan a los participantes: sin obligar a nadie, sin cerrar la puerta a nadie.

A.2 Carta de Derechos Fundamentales de la UE

Artículos 7, 8 y 11 — Privacidad, datos y libertad de información

«Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de sus comunicaciones.» / «Toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan.» / «Toda persona tiene derecho a la libertad de expresión. Este derecho incluye la libertad de opinión y la libertad de recibir o comunicar informaciones o ideas sin que pueda haber injerencia de autoridades públicas y sin consideración de fronteras.»

Carta de los Derechos Fundamentales de la Unión Europea, arts. 7, 8 y 11 (DOUE C 326, 26-10-2012)

Aplicación: los tres artículos juntos definen el equilibrio exacto del protector puro (Cap. 13): la protección cognitiva protege el *derecho a recibir información sin manipulación* (art. 11) respetando la vida privada (art. 7) y los datos personales (art. 8). El PP no filtra, no clasifica, no bloquea: la libertad de expresión queda intacta; lo que se persigue es la manipulación, no la opinión.

Artículo 47 — Tutela judicial efectiva

«Toda persona cuyos derechos y libertades garantizados por el Derecho de la Unión hayan sido violados tiene derecho a un recurso efectivo ante un tribunal, incluso en el caso de una infracción imputable a las personas que ejercen la autoridad pública.»

Carta, art. 47 (DOUE C 326, 26-10-2012)

Aplicación (alineada con el Cap. 12): toda decisión de la EDSPA y del Poder Protector es susceptible de recurso. La arquitectura de garantías del libro no crea tribunales propios: la garantía opera en tres niveles verificados — **Sala de Recurso administrativa** interna (modelo ACER), **Cámara Especializada en Protección Digital del Tribunal General**, con jueces de doble cualificación (modelo Tribunal de Patentes Unificado) y presupuesto del poder

judicial, y **casación ante el TJUE**. La jurisdicción pertenece al poder judicial; la separación de poderes es la primera garantía de diseño.

A.3 Base jurídica del Poder Protector (2033): reforma del Tratado

Artículo 48 TUE — Procedimientos de revisión

«Los Tratados podrán ser modificados conforme a un procedimiento de revisión ordinario. [...] El Gobierno de cualquier Estado miembro, el Parlamento Europeo o la Comisión podrán presentar al Consejo proyectos destinados a la modificación de los Tratados. [...] El Presidente del Consejo Europeo convocará una Convención compuesta por representantes de los Parlamentos nacionales, de los Jefes de Estado o de Gobierno de los Estados miembros, del Parlamento Europeo y de la Comisión. [...] Las modificaciones entrarán en vigor después de su ratificación por todos los Estados miembros, conforme a sus respectivas normas constitucionales.»

TUE, art. 48, apartados 1, 2 y 4 (DOUE C 326, 26-10-2012)

Aplicación (Capítulo 20): este es el camino — no una hipótesis del libro: el Parlamento Europeo lo activó formalmente el 22-nov-2023 con la resolución e informe 2022/2051(INL) sobre la reforma de los Tratados, el Consejo trasladó la petición de Convención al Consejo Europeo el 18-dic-2023, y la presidenta von der Leyen apoyó públicamente la reforma en noviembre de 2024. La cronología del libro — Convención ~2030, firma 2031-2032, PP constitucional 2033 — cabe con holgura en el precedente histórico (Laeken feb-2002 → firma oct-2004; Lisboa: 24 meses de firma a vigor).

Integración institucional: artículos 13-19 TUE

El Poder Protector se integraría en el marco institucional regulado por los **arts. 13-19 TUE**: el art. 13(1) fija que «la Unión dispone de un marco institucional que tiene por finalidad promover sus valores, perseguir sus objetivos, servir a los intereses de los ciudadanos», y el art. 13(2) exige que la Unión actúe dentro de los límites de las competencias que le atribuyen los Tratados. Un cuarto poder no es ajeno a esta arquitectura: es un nuevo rango dentro de ella, dotado por el art. 48 — con la doctrina del Cap. 15: el poder que frena al poder no multiplica al Estado, lo equilibra.

Recursos propios: artículo 311 TFUE y Decisión 2020/2053

«La Unión se dotará de los recursos necesarios para alcanzar sus objetivos y financiar sus políticas. [...] El Consejo, actuando por unanimidad de conformidad con un procedimiento legislativo especial, previa consulta al Parlamento Europeo y previa aprobación de los Estados miembros, conforme a sus respectivas normas constitucionales, establecerá nuevas categorías de recursos propios o suprimirá las categorías existentes.»

TFUE, art. 311, apartados 1 y 3 (DOUE C 326, 26-10-2012)

Aplicación (Capítulo 16): la autonomía financiera del PP tiene base textual exacta: una **Decisión de recursos propios** — como la Decisión (UE, Euratom) 2020/2053 vigente — introduce la categoría de dotación del PP con unanimidad, consulta al PE y ratificación según normas constitucionales: **el mismo procedimiento que su Tratado**, aprobado por la misma coalición fundadora. El precedente del recurso plástico (Reglamento (UE, 2021/770) desarrolló la categoría creada por la Decisión 2020/2053) muestra la mecánica completa.

A.4 El acervo regulatorio que la EDSPA y el PP hacen ejecutivo

Acto	Referencia oficial	Rol de la EDSPA / del PP (protector puro)
Reglamento de Servicios Digitales (DSA)	Reglamento (UE) 2022/2065; auditorías independientes anuales del art. 37 (primera ronda exigida en ago-2024, Reglamento Delegado (UE) 2024/436); acceso de investigadores del art. 40 (acto delegado, 2-jul-2025); sanciones de hasta el 6% de la facturación mundial anual (Comisión/autoridades DSA)	Audita la manipulación en plataformas, genera evidencia forense y remite expedientes a la Comisión y autoridades nacionales — la sanción es de ellas, nunca del PP (Caps. 12-13)
Ley de Inteligencia Artificial (AI Act)	Reglamento (UE) 2024/1689, de 13-jun-2024; aplicación plena desde el 2-ago-2026; sanciones de hasta el 7%	Auditoría algorítmica y evidencia sobre sistemas de IA de manipulación; remisión a los supervisores del AI Act
RGPD	Reglamento (UE) 2016/679, de 27-abr-2016	La esfera cognitiva se compone de datos personales: sus garantías son el suelo, no el techo
Reglamento de Datos (Data Act)	Reglamento (UE) 2023/2854; aplicable desde el 12-sep-2025	Acceso a datos y cambio de proveedor de servicios en la nube: condiciones prácticas de la auditoría
Programa del Decenio Digital	Decisión (UE) 2022/2481 (objetivos 2030: 20M especialistas TIC, 80% competencias básicas, 75% empresas cloud/IA)	La función educativa del PP sirve las metas oficiales de alfabetización de la Unión
Escudo Europeo de la Democracia	Comunicación de la Comisión, 12-nov-2025	El marco de protección electoral de la Unión: la EDSPA aporta el brazo forense especializado
Paquete de Soberanía Tecnológica Europea	Comisión Europea, 3-jun-2026 (semiconductores, IA, nube y open source)	El marco estratégico de independencia tecnológica en el que encajan las tres fases del Cap. 18
Precedente de transición	Reglamento (UE) 2016/794 (Europol): la agencia sucesora asume el personal y las funciones por acto de organización	Modelo del acto de organización sucesora para la integración EDSPA→PP 2033-2035 sin vacío legal (Cap. 14)

A.5 Jurisprudencia del TJUE: la protección como doctrina consolidada

- **Digital Rights Ireland (C-293/12 y C-294/12, 8-abr-2014)**: el TJUE anuló la Directiva de Retención de Datos porque la interferencia de la vida privada «debe limitarse a lo estrictamente necesario» — la fundamentación jurídica de que *más vigilancia no es más seguridad*: la doctrina exacta que separa al protector del vigilante.
- **Google Spain (C-131/12, 13-may-2014)**: el derecho de supresión frente al buscador: el individuo tiene derechos efectivos frente a los operadores digitales, base de la tradición que el Comprobador Ciudadano (Cap. 13) extiende a la verificación de indicios.
- **Schrems II (C-311/18, 16-jul-2020)**: invalidación del Privacy Shield por transferencias de datos a terceros países: la soberanía de datos personales es jurisprudencia, no eslogan — y la motivación profunda de que la evidencia forense europea deba tratarse en infraestructura europea (Cap. 18).
- **ACER (C-46/21 P, 2023)**: el modelo validado de la Sala de Recurso administrativa dentro de una agencia — la primera línea de garantía del Cap. 12.

A.6 Marco global: el mundo ya escribió la doctrina

- **Convenio Marco del Consejo de Europa sobre IA** (abierto a firma 5-sep-2024, Vilna): primer tratado internacional jurídicamente vinculante sobre IA y derechos humanos, democracia y Estado de derecho — firmado por la Comisión en nombre de la UE.
- **Principios Globales de la ONU para la Integridad de la Información** (Guterres, 24-jun-2024): la doctrina global contra la manipulación potenciada por IA.
- **Principios OCDE sobre IA** (2019, actualizados may-2024): el primer estándar intergubernamental de IA fiable.

La doctrina global existe y está escrita por terceros; lo que no existe es la institución permanente que la encarne. Ese es el hueco — y la oportunidad — que el libro demuestra (Cap. 21).

A.7 Resumen de la base jurídica

Institución	Base legal	Procedimiento	Garantía clave
EDSPA (2027-2030)	Arts. 114, 16, 352 TFUE; cooperación reforzada art. 20 TUE + arts. 326-334 TFUE	Reglamento ordinario; cooperación reforzada con núcleo de 9 Estados como último recurso	Sin reforma del Tratado; abierta en todo momento al resto (art. 331 TFUE)
Poder Protector (2033)	Art. 48 TUE (revisión ordinaria, ya activada por el PE 22-nov-2023); arts. 13-19 TUE; art. 311 TFUE (recursos propios)	Convención → CIG → unanimidad → ratificación por los 27 según sus normas constitucionales	Permanencia constitucional + autonomía financiera con el mismo procedimiento que el Tratado

A.8 Referencias oficiales

- **Tratados consolidados:** TUE, TFUE y Carta de los Derechos Fundamentales de la UE, versiones consolidadas, DOUE C 326, 26-10-2012 (los textos citados corresponden a esta consolidación).
- **Estado real de la revisión:** PE, resolución e informe 2022/2051(INL), 22-nov-2023 (activación del art. 48(2) TUE); traslado del Consejo al Consejo Europeo, 18-dic-2023; apoyo público de von der Leyen, nov-2024.
- **Legislación citada:** Reglamentos (UE) 2022/2065 (DSA), 2024/1689 (AI Act), 2016/679 (RGPD), 2023/2854 (Data Act); Decisiones (UE) 2022/2481 (Decenio Digital) y (UE, Euratom) 2020/2053 (recursos propios); Reglamento (UE) 2021/770 (recurso plástico); Reglamento (UE) 2016/794 (Europol).
- **Jurisprudencia:** TJUE, sentencias C-293/12 y C-294/12 (Digital Rights Ireland, 2014), C-131/12 (Google Spain, 2014), C-311/18 (Schrems II, 2020), C-46/21 P (ACER, 2023).
- **Marco global:** Convenio Marco del Consejo de Europa sobre IA (5-sep-2024); Principios Globales de la ONU para la Integridad de la Información (24-jun-2024); Principios OCDE sobre IA (2019/2024).
- **Actos de 2025-2026:** Escudo Europeo de la Democracia (Comunicación, 12-nov-2025); Paquete de Soberanía Tecnológica Europea (3-jun-2026).

Anexo B: Capacidades Operativas del Protector Puro

Qué podrá hacer la institución — y lo que deliberadamente este anexo no dice: la regla del libro («hitos y resultados, nunca procedimientos ni técnicas») se aplica primero al propio libro

Propósito del anexo

La tentación será describir un sistema completo — arquitecturas por capas, modelos con nombre y parámetros, marcas comerciales, volúmenes de datos y mecanismos de «neutralización». Este anexo hace exactamente lo contrario — y por una razón de doctrina, no de discreción casual: **el libro exige al Poder Protector publicar hitos y resultados, nunca procedimientos ni técnicas** (Caps. 18-19), porque la esfera cognitiva es un dominio adversarial y cada detalle metodológico publicado es capacidad regalada al rival. La regla que la institución deberá cumplir, este libro la cumple ya. Lo que sigue es, por tanto, un anexo de **capacidades**: qué podrá hacer la institución, con qué garantías y contra qué amenazas — no cómo lo hará. Las capacidades se anclan en los marcos técnicos reales ya existentes (NIST, ISO/IEC, ENISA, SEAE, DSA/AI Act) que la institución haría operativos.

B.1 La doctrina del anexo: lo que este documento no dice

El criterio que gobierna cada sección es el de la Cláusula de Aceleración y del radar anual del Capítulo 18: **el interior íntegro, el exterior sintético**. Aplicado a un anexo técnico, significa que se publican:

- **Capacidades** — qué puede hacer la institución (detectar, auditar, publicar, remitir, educar).
- **Garantías** — qué límites de diseño la hacen digna de confianza (doble verificación, transparencia por defecto, privacidad desde el diseño).
- **Taxonomías** — cómo se clasifican las amenazas, porque la clasificación pública educa al ciudadano y no regala nada.

Y no se publican: modelos con parámetros, stacks tecnológicos, herramientas, volúmenes de datos, metodologías de auditoría paso a paso, umbrales operativos internos ni plazas de respuesta automatizada. Publicar todo eso será un error doble: **revelar la caja negra del protector ante la industria de la manipulación**.

B.2 Capacidades nucleares

Capacidad	Qué hace	Qué produce (hitos y resultados)	Qué nunca hace
Escáner forense cognitivo (Caps. 8 y 13)	Detecta patrones de manipulación en la esfera pública digital y genera evidencia	Evidencia forense auditable y reproducible, con doble verificación humano-IA	No filtra, no clasifica la verdad, no bloquea contenido
Auditoría algorítmica (Cap. 13)	Audita sistemas y plataformas dentro del acervo (DSA, AI Act)	Informes públicos, evidencia reproducible, expedientes de remisión a la Comisión y autoridades nacionales	No sanciona — ni propia ni delegadamente; la sanción es de la Comisión/autoridades (6% DSA, 7% AI Act)
Educación cognitiva (Cap. 12)	Alfabetización de la ciudadanía al servicio de las metas del Decenio Digital (80% competencias, 20M especialistas TIC en 2030)	Programas, materiales y métricas públicas de alfabetización (objetivo del libro: ≥90% en 2038)	No induce, no persuade: enseña a reconocer la manipulación de cualquier signo
Inteligencia de amenazas (Cap. 18)	Radar anual «Estado de la Carrera Cognitiva»: interior íntegro, resumen público sintético	Publica tendencias, hitos y resultados; la base de evidencia es un bien público global (Cap. 21)	No publica técnicas de detección ni fuentes ni métodos
Comprobador Ciudadano (Cap. 13)	Verificación no vinculante de indicios aportados por el ciudadano, con pseudonimización	Respuesta verificada al ciudadano; estadísticas agregadas públicas	Sin vínculo reversible a la identidad; sin servicio antes de su evaluación 2033-2035

B.3 Clasificación de amenazas (taxonomía pública)

Niveles de amenaza y respuesta del protector puro

La taxonomía por gravedad es material educativo público; la columna de respuesta sigue íntegramente las cinco funciones del Cap. 13 — detectar, auditar, publicar, remitir, educar. El PP no neutraliza, retira ni suspende nada.

Nivel	Descripción	Ejemplo	Respuesta del protector puro
Crítico	Amenaza existencial para un proceso democrático	Interferencia electoral masiva coordinada	Detección prioritaria, publicación inmediata de evidencia, remisión urgente a las autoridades competentes (Comisión electoral/DSA, Estados)
Alto	Amenaza grave con impacto significativo	Campaña FIMI coordinada contra un Estado miembro	Auditoría forense, informe público y expediente de remisión
Medio	Amenaza moderada con impacto limitado	Desinformación localizada	Detección, evidencia en el archivo público, educación dirigida
Bajo	Amenaza menor con impacto mínimo	Contenido engañoso aislado	Monitoreo y alimentación del archivo de evidencia

Tipos de amenaza

Tipo	Ejemplos	Referencia de taxonomía real
Desinformación y engaño sintético	Noticias falsas, deepfakes, imágenes manipuladas	Clasificación FIMI del SEAE; informes de amenazas de ENISA (2023: la IA y los LLM como vectores de desinformación e ingeniería social)
Manipulación algorítmica	Burbujas, microsegmentación, amplificación por redes de bots	Obligaciones de transparencia y riesgo del DSA (Reglamento (UE) 2022/2065); AI Act (Reglamento (UE) 2024/1689) sobre sistemas de manipulación
FIMI estatal	Infraestructura de manipulación extranjera (Rusia, China mapeadas por el SEAE)	3er Informe FIMI del SEAE (2024): infraestructura digital desplegada contra el espacio informativo europeo
Ciberamenaza a la esfera	Phishing, ransomware, DDoS contra medios y procesos electorales	ENISA Threat Landscape (2.580 incidentes jul-2022/jun-2023; la administración pública, el sector más golpeado)

Matriz de priorización

Gravedad \ Probabilidad	Baja	Media	Alta
Baja	Monitoreo	Monitoreo	Evidencia pública
Media	Monitoreo	Evidencia pública	Informe y educación
Alta	Evidencia pública	Informe y remisión	Publicación inmediata + remisión urgente

La matriz sigue el espectro del protector puro: monitoreo → evidencia pública → informe → remisión. El arma del PP es la luz; los plazos y umbrales concretos son materia del reglamento interno, no de un anexo publicado.

B.4 Capacidades de auditoría — resultados, no procedimientos

El anexo enuncia solo el resultado: toda auditoría del PP produce **tres artefactos públicos** — un **informe** (conclusiones y evidencia), **evidencia reproducible** (verificable por terceros, con doble verificación humano-IA) y, si hay indicio de infracción, un **expediente de remisión** a quien tiene el poder sancionador. El procedimiento es patrimonio interno y estándar profesional; el resultado es público por diseño.

Los requisitos que la institución sí declara — porque son garantía para el ciudadano, no capacidad para el rival — son los del Capítulo 18: toda IA propia será **abierta, auditable y explicable**, con doble verificación humana no automatizable; y toda adquisición se hará por **convocatoria abierta**, sin dependencia de un único proveedor (lección Gaia-X del Cap. 18).

B.5 Garantías de diseño (lo auditable es siempre lo humano)

- **Doble verificación humano-IA (Cap. 8):** ninguna actuación institucional relevante nace ni muere en la máquina; el criterio humano firma. Esta es la respuesta de diseño a la paradoja del 60% (Cap. 19): la desconfianza ciudadana es la condición del poder, no su riesgo.
- **Transparencia por defecto:** art. 15(3) TFUE y Reglamento 1049/2001: los documentos son públicos salvo excepción motivada; el Informe Anual de Protección Cognitiva ante el Parlamento es la rendición de cuentas estructural (Cap. 19).
- **Privacidad desde el diseño:** RGPD art. 25 y minimización de datos; la vigilancia es jurídicamente imposible por arquitectura (Digital Rights Ireland: la interferencia «debe limitarse a lo estrictamente necesario» — Anexo A.5).
- **Simetría anti-arma (Cap. 13):** las mismas herramientas que protegen al ciudadano de la manipulación no pueden usarse para manipularlo; el límite es constitucional, no programático.
- **Separación detectar/sancionar (Caps. 9, 12-13):** el PP detecta y publica; la Comisión y las autoridades sancionan. Ningún porcentaje de multa financia al PP: las multas van a las arcas de la UE (Cap. 16).

B.6 Interfaces públicas

Interfaz	Público	Contenido
Informe Anual de Protección Cognitiva (24 lenguas, ante el PE — Cap. 19)	Toda la Unión	Hitos y resultados, nunca procedimientos ni técnicas
Portal de evidencia	Investigadores, medios, ciudadanos	Evidencia forense reproducible de casos cerrados
Alertas verificadas	Ciudadanía	Avisos de campañas activas con evidencia, sin alarma ni censura
Datos abiertos y educación	Sistema educativo, Estados	Taxonomías, materiales de alfabetización, métricas agregadas

El precedente de acceso ya existe y es verificable: el acto delegado de jul-2025 del **art. 40 DSA** permite a investigadores acreditados acceder a datos no públicos de las plataformas — la institución conectaría esa evidencia dispersa en un archivo público sistemático.

B.7 Marcos técnicos de referencia (reales y verificables)

- **NIST AI Risk Management Framework (AI RMF 1.0, NIST AI 100-1, ene-2023)** y su **perfil de IA generativa (NIST AI 600-1, jul-2024)**: el estándar de gestión de riesgos de IA más adoptado del mundo — la columna vertebral metodológica que la institución haría operativa sin publicar.
- **ISO/IEC 42001:2023** (dic-2023): el primer estándar internacional de sistema de gestión de IA (AIMS) — el marco de gobernanza bajo el que se certificaría la IA propia.
- **ENISA**: Threat Landscape anual (2.580 incidentes jul-2022/jun-2023) y el mapa de amenazas de IA — la línea base europea de ciberamenaza que alimenta la taxonomía de B.3.
- **SEAE, informes FIMI** (1º-3º, el tercero de 2024): la clasificación de referencia europea de manipulación informativa extranjera.
- **DSA arts. 37** (auditorías anuales independientes a cargo de las plataformas, primera ronda ago-2024) y **40** (acto delegado jul-2025 de acceso para investigadores verificados) y **AI Act art. 6** y anexos (evaluación y supervisión de sistemas de alto riesgo): el acervo que la auditoría del PP haría sistemático.

Anexo C: Estudios de Caso

Propósito y método

Este anexo examina episodios reales de amenaza a la esfera cognitiva y las respuestas institucionales que existieron, para extraer las lecciones de diseño que justifican a la EDSPA y al Poder Protector. La regla del anexo: **solo cifras verificadas** — este anexo enuncia lo cualitativo verificable o cita el dato con su origen real. Y las «conexiones con el Poder Protector» se reformulan a la doctrina del protector puro: **el PP no sanciona ni neutraliza — genera evidencia forense pública, remite expedientes y educa.**

C.1 Amenazas: seis episodios reales

1. Desinformación en las elecciones europeas (2019)

Contexto: las elecciones al Parlamento Europeo (23-26 mayo 2019) se celebraron con campañas coordinadas de desinformación anti-UE y de polarización, con cuentas falsas y amplificación de narrativas divisivas, documentadas por el SEAE y las plataformas.

Respuesta real: la **East StratCom Task Force** del SEAE (creada en 2015) mantiene EUvsDisinfo, la base de datos pública de casos de desinformación desmentidos desde 2015; las plataformas eliminaron redes de cuentas y publicaron informes de transparencia electoral; los verificadores de hechos cubrieron la campaña.

Lecciones para el PP (protector puro): la respuesta existente fue *observacional* (desmentir) y *plataforma por plataforma* (retirar cuentas): nadie generó evidencia forense sistemática ni un archivo público europeo unificado. El PP habría aportado exactamente eso: detección forense, evidencia reproducible y remisión coordinada — sin sustituir a nadie.

2. Síntesis engañosa en las elecciones de EE.UU. (2020)

Contexto: las presidenciales de 2020 se acompañaron de manipulación sintética de vídeo e imagen y de narrativas sobre el fraude electoral que erosionaron la confianza en el resultado.

Respuesta real: CISA (la agencia federal de ciberseguridad de infraestructura electoral) y las plataformas mantuvieron sistemas de etiquetado y retirada; los verificadores trabajaron durante el ciclo completo.

Lecciones para el PP: la detección llegó siempre *después* de la viralidad, y la acción dependió de las propias plataformas — el mismo diagnóstico de dependencia del Capítulo 4. Un archivo forense europeo de síntesis engañosa, con evidencia verificable y doble verificación humana, habría hecho auditable lo que cada plataforma afirmaba en solitario.

3. Manipulación algorítmica: Cambridge Analytica y el Brexit (2016-2018)

Contexto: Cambridge Analytica explotó los datos de hasta **87 millones de perfiles de Facebook**, obtenidos sin consentimiento informado mediante una aplicación, para publicidad política microsegmentada en campañas de varios países, alrededor del referéndum del Reino Unido (23-jun-2016).

Consecuencias verificadas: la ICO británica multó a Facebook con **£500.000** (oct-2018) por la infracción grave de protección de datos, y la **FTC estadounidense con \$5.000 millones** (jul-2019), una de las mayores multas de la historia de la privacidad.

Lecciones para el PP: el caso demostró que la microsegmentación manipulativa funciona a escala industrial *antes* de que ningún regulador lo sepa — y que la evidencia llegó por periodismo y denuncia interna, no por auditoría institucional. La auditoría algorítmica del PP (Cap. 13) existe para que el próximo Cambridge Analytica no se descubra por casualidad: detección temprana, evidencia pública, remisión a las autoridades de protección de datos y de competencia.

4. Desinformación en la pandemia de COVID-19 (2020-2021)

Contexto: campañas de desinformación sobre el origen del virus y las vacunas, amplificadas por actores estatales y comunitarios, con efecto documentado de vacilación vacunal y polarización.

Respuesta real: la OMS acuñó la «infodemia» y coordinó campañas de información verificada; la UE desplegó a EDMO (2020) y su red de verificadores; Facebook reportó haber retirado **más de 12 millones de piezas de contenido** sobre COVID-19 entre marzo y octubre de 2020 (dato propio de la plataforma) y más de 20 millones hasta mediados de 2021.

Lecciones para el PP: la respuesta fue global en diagnóstico y fragmentada en acción: cada plataforma decidió qué retirar, sin evidencia pública verificable del criterio. La función educativa del PP — alfabetización cognitiva permanente, no campañas de emergencia — es la respuesta estructural a la infodemia.

5. Interferencia en las elecciones de Francia (2022)

Contexto: en las presidenciales de abr-2022, Francia desplegó por primera vez un servicio dedicado: **Viginum** (creado en 2021), el servicio de vigilancia y protección contra las interferencias digitales extranjeras.

Respuesta real: Viginum detectó y **publicó informes de manipulación informativa** (incluidas redes coordinadas de origen extranjero) durante el ciclo electoral, coordinando con ANSSI, la CNIL y las plataformas; la publicación de la evidencia fue parte esencial de la respuesta.

Lecciones para el PP: Francia probó en miniatura la tesis del libro: un organismo pequeño, dedicado, que *detecta y publica*, cambia la calidad de la respuesta sin necesidad de poderes sancionadores propios. El PP es esa idea elevada a escala europea y a rango constitucional — con permanencia y recursos propios, y sin la fragilidad de un servicio dependiente del ciclo político.

6. Desinformación en las elecciones de Brasil (2022-2024)

Contexto: las presidenciales de 2022 vivieron desinformación masiva, ataques a los sistemas electorales y un asalto a las instituciones el 8-ene-2023 tras meses de negación del resultado.

Respuesta real: el TSE (Tribunal Superior Electoral) operó un modelo agresivo de retirada rápida con orden judicial y acordó protocolos con las plataformas; para las municipales de 2024 prohibió el uso de deepfakes electorales (con etiquetado obligatorio del contenido de IA) y firmó memorandos con Meta, TikTok y otras plataformas; investigaciones documentaron pagos encubiertos de RT a influencers.

Lecciones para el PP: el modelo brasileño demuestra dos cosas: que la acción rápida es posible — pero concentrada en un poder judicial electoral nacional, con los problemas de transparencia que ello genera (criticados por la propia prensa brasileña), y sin arquitectura de evidencia pública verificable. El PP aportaría lo que falta: evidencia forense reproducible y transparencia por defecto, en lugar de retiradas opacas.

C.2 Modelos de respuesta institucional: lo que existe y lo que enseña

Modelo	Creación	Dato verificado	Lección para el PP
ANSSI (Francia)	2009	Agencia nacional de ciberseguridad; respuesta a incidentes y protección de infraestructuras críticas	La especialización técnica funciona; su límite es el ámbito (ciberseguridad, no esfera cognitiva)
NCSC (Reino Unido)	2016	Centro técnico nacional de ciberseguridad, modelo de coordinación público-privada y transparencia operativa	Una agencia técnica (no política) publicando abiertamente gana la confianza del sector
ENISA (UE)	2004	Presupuesto verificado ~€26,9M (Cap. 6); estándares y certificación para los 27	La agencia europea de referencia demuestra la viabilidad de la coordinación UE — y su presupuesto mínimo muestra el techo de lo que NO puede hacerse barato (Cap. 11: fragilidad institucional)
EDMO (UE)	2020	Observatorio y red de verificadores; la financiación de sus hubs termina en 2026 sin sucesor garantizado (Cap. 11)	El monitoreo sin permanencia ni capacidad ejecutiva es un parche que se desprende: exactamente el hueco que la EDSPA llena
Viginum (Francia)	2021	Servicio dedicado a interferencias digitales extranjeras; detecta y publica informes	El precedente directo del protector puro en miniatura: evidencia pública sin poder sancionador — nacional, pequeño y temporal; el PP lo hace europeo, permanente y dotado

C.3 Indicadores verificados de la amenaza (2019-2026)

Este anexo utiliza los indicadores verificados que el libro ya utiliza (Cap. 19 y Parte I):

Indicador	Dato verificado	Fuente
Preocupación ciudadana por la desinformación	69% la considera un problema; 36% expuesto «a menudo» (28% en 2022); 85% en España	Eurobarómetro desinformación 2025 (36%, exposición); Eurobarómetro feb-2026 (69%, preocupación)
Confianza en las noticias	37%, mínimo desde 2015; avoidance informativo 42% (29% en 2017); las redes superan a la TV como fuente	Reuters Institute Digital News Report 2026
Insularidad informativa	7/10 ciudadanos viven en cámaras de eco	Edelman Trust Barometer 2026 (34.000 encuestados, 28 países)
Infraestructura FIMI extranjera	Mapa de la infraestructura digital desplegada principalmente por Rusia y también China contra el espacio informativo europeo	3er Informe FIMI del SEAE (2024)
Desconfianza en la IA gubernamental	60% desconfía del uso gubernamental de la IA — frente al 69% que exige protección	OECD Trust Survey, jun-2026 (la paradoja del 60%, Cap. 19)

Tendencias cualitativas verificables (sin series numéricas inventadas): la migración del flujo informativo hacia plataformas más opacas y menos moderadas (TikTok, Telegram, X); la aceleración de la producción de contenido sintético por la IA generativa (Stanford AI Index 2026); y la convergencia de todos los modelos institucionales hacia la publicación de evidencia — el campo al que el PP llega primero.

C.4 El patrón que los seis casos dibujan

En todos los casos se repite la misma secuencia: detección tardía (cuando el daño ya viralizó) → evidencia no forense (afirmaciones de plataformas sin verificación independiente) → respuesta fragmentada (cada actor con su criterio, cada país con su ley) → ninguna institución permanente responsable de aprender del caso. **El Poder Protector es la corrección institucional de esa secuencia:** detección forense permanente, evidencia pública y reproducible, remisión coordinada a los sancionadores, y memoria institucional — un archivo europeo de cómo se manipula y de cómo se resiste (Cap. 21: un bien público global que nadie más producirá).

C.5 Fuentes y referencias verificadas

- **SEAE:** East StratCom Task Force (2015) y EUvsDisinfo (base de datos pública de casos desmentidos); 3er Informe FIMI (2024).
- **Cambridge Analytica:** ICO, multa de £500.000 a Facebook (oct-2018); FTC, acuerdo de \$5.000 millones (jul-2019); datos de hasta 87 millones de perfiles documentados en ambas actuaciones.
- **COVID-19:** OMS («infodemia»); EDMO (2020); cifras de retirada reportadas por Facebook/Meta (más de 12 millones de piezas mar-oct-2020; más de 20 millones hasta mediados de 2021).
- **Francia:** Viginum (creado 2021), informes públicos de manipulación informativa en el ciclo 2022; ANSSI.
- **Brasil:** TSE, protocolos con plataformas (2022), prohibición de deepfakes electorales y memorandos con Meta/TikTok y otras (2024); investigación sobre pagos de RT a influencers.
- **Indicadores:** Eurobarómetro feb-2026; Reuters Institute Digital News Report 2026; Edelman Trust Barometer 2026; OECD Trust Survey jun-2026; Stanford AI Index 2026.
- **Parlamento Europeo:** trabajos de la comisión especial INGE sobre interferencia extranjera (2020-2022).

Anexo D: Bibliografía

D.1 El criterio de esta bibliografía

La bibliografía aplica al aparato de fuentes la misma regla que aplica al resto del libro: **ninguna fuente se cita por su prestigio aparente, sino por su verificación**. Cada documento de esta lista ha sido comprobado en su publicación oficial (EUR-Lex, portal institucional del emisor o editorial de referencia). Esta bibliografía cumple tres funciones:

1. **Respaldo:** toda afirmación factual del libro tiene aquí su fuente.
2. **Rastreabilidad:** el lector puede ir de cualquier cifra a su documento de origen.

D.2 Tratados y documentos constitucionales de la UE

Documento	Artículos citados	Referencia
Tratado de la Unión Europea (TUE)	Arts. 2, 3, 13-19, 20, 42.7, 48	Versión consolidada, DOUE C 326, 26/10/2012
Tratado de Funcionamiento de la UE (TFUE)	Arts. 16, 114, 222, 311, 326-334, 352	Versión consolidada, DOUE C 326, 26/10/2012
Carta de los Derechos Fundamentales de la UE	Arts. 2, 7, 8, 11, 47	Versión consolidada, DOUE C 326, 26/10/2012
Resolución del Parlamento Europeo 2022/2051(INL)	Propuestas de reforma de los Tratados; activación del art. 48(2) TUE	Aprobada el 22 de noviembre de 2023
Decisión (UE, Euratom) 2020/2053	Sistema de recursos propios; base del art. 311 TFUE	DOUE L 424, 15/12/2020
Reglamento (UE, Euratom) 2021/770	Recurso propio plástico: cálculo del recurso propio basado en los residuos de envases de plástico no reciclados; desarrolla la categoría creada por la Decisión 2020/2053 (art. 311 TFUE)	DOUE L 165, 11/5/2021

Nota de rigor: el Reglamento (UE, Euratom) 2021/770 desarrolla el recurso propio plástico creado por la Decisión 2020/2053: el precedente del libro de una categoría de recursos propios introducida por Decisión (art. 311 TFUE) y puesta en marcha por reglamento (Anexo A.3). No es base jurídica de la EDSPA. Verifíquese siempre el alcance real de cada norma antes de extenderla por analogía.

D.3 Derecho derivado: el acervo digital europeo

Instrumento	Materia	Referencia
Reglamento sobre un Mercado Único de Servicios Digitales (DSA)	Responsabilidad de plataformas; art. 40 (acto delegado, julio 2025)	Reglamento (UE) 2022/2065
Reglamento de Inteligencia Artificial (AI Act)	Normas armonizadas sobre IA	Reglamento (UE) 2024/1689
Reglamento General de Protección de Datos (RGPD)	Protección de datos; art. 25 (privacidad por diseño)	Reglamento (UE) 2016/679
Reglamento de Datos (Data Act)	Acceso y compartición de datos	Reglamento (UE) 2023/2854
Decisión relativa al Programa «Decenio Digital 2030»	Objetivos digitales 2030 (20M especialistas TIC, 80% competencias básicas, 75% empresas cloud/IA)	Decisión (UE) 2022/2481
Reglamento de Europol	Precedente de agencia para la transición	Reglamento (UE) 2016/794
Escudo Europeo de la Democracia	Comunicación de la Comisión	12 de noviembre de 2025
Paquete de Soberanía Tecnológica	Iniciativa de la Comisión	3 de junio de 2026

D.4 Jurisprudencia del Tribunal de Justicia de la UE

Sentencia	Año	Aporte al libro
Digital Rights Ireland (asuntos acumulados C-293/12 y C-294/12)	2014	Invalidó la Directiva de Retención de Datos: la privacidad es la regla, su injerencia la excepción tasada
Google Spain (C-131/12)	2014	Creó el derecho de supresión: el interesado prevalece sobre el buscador
Schrems II (C-311/18)	2020	La protección de datos europeos viaja con los datos: la soberanía digital es exigible extraterritorialmente
ACER (C-46/21 P)	2023	Modelo de Sala de Recurso administrativa de agencia con recurso judicial ulterior

D.5 Informes estratégicos 2024-2026

Informe	Autor/Año	Aporte al libro
«La competitividad futura de Europa» (informe Draghi)	Comisión Europea, 2024	Diagnóstico de la brecha de productividad y la dependencia tecnológica
«Mucho más que un mercado» (informe Letta)	2024	El mercado único como palanca pendiente; el mercado único de datos
Informe Niinistö sobre la seguridad y resiliencia de la UE	2024	Comprender, anticipar y preparar: la seguridad como función permanente
Tercer informe sobre amenazas FIMI	Servicio Europeo de Acción Exterior (SEAE), 2024	Taxonomía de interferencia extranjera en espacios informativos
ENISA Threat Landscape	Agencia de la UE para la Ciberseguridad (ENISA)	2.580 incidentes notificados jul-2022/jun-2023
Escudo Europeo de la Democracia y Paquete de Soberanía Tecnológica	Comisión Europea, 2025-2026	La protección de la esfera informativa ya es política oficial de la UE

D.6 Datos, encuestas y sondeos

Fuente	Dato citado	Detalle
Eurobarómetro sobre desinformación (edición 2025)	36% expuesto «a menudo» o «muy a menudo» en los últimos 7 días (28% en 2022)	Publicado por la Comisión Europea, campo 2025
Eurobarómetro sobre desinformación (publicado feb-2026)	69% considera la desinformación un problema en su país; 85% en España	Publicado por la Comisión Europea, campo de otoño de 2025
Reuters Digital News Report	Confianza en noticias y consumo digital	Edición 2026, Reuters Institute, Universidad de Oxford
OECD Survey on Drivers of Trust in Public Institutions — 2026 Results	~60% de confianza media-baja en el uso gubernamental de la IA; base de la paradoja del 60%	OECD Publishing, 2026
Edelman Trust Barometer	Tendencias de confianza institucional	Edición 2026

Nota de rigor: la paradoja del 60% (Capítulo 19) se construye con datos del Eurobarómetro de febrero de 2026 y de la OCDE, atribuidos a su fuente y año. Si una edición posterior revisara las cifras, el argumento no cambia: lo relevante es la brecha entre la demanda de protección y la desconfianza hacia quien protege, que ambas series capturan por separado.

D.7 Normas y estándares técnicos

Norma	Organización	Detalle
AI Risk Management Framework 1.0 (AI RMF 1.0)	NIST (EE. UU.)	Enero de 2023
Generative AI Profile (NIST AI 600-1)	NIST	Julio de 2024
ISO/IEC 42001:2023	ISO/IEC	Primer sistema de gestión de IA certifiable, diciembre de 2023
Principios de IA de la OCDE	OCDE	2019, actualizados en mayo de 2024

D.8 Marco internacional de protección de la información

Instrumento	Fecha	Aporte al libro
Principios Globales de las Naciones Unidas para la Integridad de la Información	24 de junio de 2024	El Secretario General llama a un ecosistema informativo sano; deriva de «Nuestra Agenda Común» (2021), base de la Cumbre del Futuro (septiembre de 2024)
Convenio Marco del Consejo de Europa sobre Inteligencia Artificial	Abierto a firma el 5 de septiembre de 2024 (Vilna)	Primer tratado vinculante mundial sobre IA; firmado por la Comisión en nombre de la UE

D.9 Literatura académica

Obras reales, publicadas por editoriales académicas, citadas en el libro por su análisis — no por la autoridad de sus autores:

Autor/a	Año	Obra	Editorial
Zuboff, Shoshana	2019	The Age of Surveillance Capitalism	PublicAffairs
Morozov, Evgeny	2011	The Net Delusion	PublicAffairs
Morozov, Evgeny	2013	To Save Everything, Click Here	PublicAffairs
Pariser, Eli	2011	The Filter Bubble	Penguin Press
Sunstein, Cass R.	2017	#Republic: Divided Democracy in the Age of Social Media	Princeton University Press
Nye, Joseph S.	2004	Soft Power: The Means to Success in World Politics	PublicAffairs
Wardle, Claire y Derakhshan, Hossein	2017	Information Disorder: Toward an Interdisciplinary Framework	Consejo de Europa

D.10 Portal de verificación

- **EUR-Lex:** eur-lex.europa.eu — textos consolidados de tratados y derecho derivado
- **Comisión Europea:** ec.europa.eu — comunicaciones, estrategias y Eurobarómetros
- **Parlamento Europeo:** europarl.europa.eu — resoluciones y actas
- **Consejo:** consilium.europa.eu — conclusiones
- **Tribunal de Justicia de la UE:** curia.europa.eu — jurisprudencia
- **OCDE:** oecd.org — encuestas de confianza y principios de IA
- **NIST:** nist.gov — marcos de gestión de riesgos de IA

Anexo E: Glosario

E.1 Cómo usar este glosario

Cada entrada refleja **exactamente** el uso del término en el cuerpo del libro. Cuando una definición depende de una cifra, la cifra es la verificada en el capítulo correspondiente.

E.2 Términos fundamentales

Término	Definición V3
Esfera Cognitiva Digital	El entorno en el que los ciudadanos interactúan con información, ideas y narrativas a través de medios digitales: redes sociales, buscadores, plataformas de comunicación y sistemas de IA. Es el ámbito que el libro declara digno de protección constitucional.
Protección Cognitiva	Conjunto de medidas, herramientas y políticas para proteger la esfera cognitiva digital de la desinformación, la manipulación algorítmica y los deepfakes. Es el objeto del Poder Protector y de la EDSPA.
Desinformación	Información falsa o engañosa creada y difundida deliberadamente. El libro adopta la taxonomía del Consejo de Europa (Wardle y Derakhshan, 2017) que distingue misinformation (falso, sin intención de dañar), disinformation (falso, con intención) y malinformation (verdadero, difundido con intención de dañar).
FIMI	Foreign Information Manipulation and Interference: interferencia y manipulación informativa extranjera. Término acuñado por el Servicio Europeo de Acción Exterior, que publica informes anuales de amenazas (tercer informe, 2024).
Deepfake	Contenido sintético (imagen, audio, vídeo) generado por IA que parece real pero muestra personas o hechos que no ocurrieron.
Manipulación Algorítmica	Uso de algoritmos para influir en el comportamiento o las opiniones de forma oculta o no transparente; incluye burbujas de filtro y priorización engañosa de contenido.
Soberanía Digital	Capacidad de un país o región para controlar su infraestructura digital, sus datos y sus tecnologías sin dependencia de actores externos. Objetivo estratégico de la UE confirmado por el Paquete de Soberanía Tecnológica (3 de junio de 2026).
Efecto Bruselas	Mecanismo por el que la regulación europea se convierte en estándar de facto global porque las empresas aplican en todo el mundo lo que deben cumplir en el mercado único. Precedente clave para la proyección internacional del modelo europeo (RGPD).

E.3 Términos institucionales

Término	Definición V3
Poder Protector (PP)	Propuesta de 4º poder constitucional de la UE: institucionaliza la protección de la esfera cognitiva con dotación estable, garantías jurisdiccionales y alcance europeo. No sustituye a los poderes existentes: audita, publica, remite y educa.
Protector Puro	Doctrina operativa del PP: detecta, publica, remite y educa; nunca neutraliza, retira ni sanciona . La separación entre quien detecta la evidencia y quien decide las consecuencias es la garantía central contra el abuso.
EDSPA	European Digital Sphere Protection Agency (Agencia Europea de Protección de la Esfera Digital). Agencia de transición 2027-2030 creada por cooperación reforzada con 9 Estados fundadores; sentará las bases técnicas y de confianza del Poder Protector.
Sala de Recurso administrativa	Garantía de recurso dentro de la agencia, según el modelo ACER validado por el TJUE (C-46/21 P), con ulterior control jurisdiccional.
Cámara Especializada del Tribunal General	Instancia de control jurisdiccional especializada en protección cognitiva, con casación ante el TJUE: el PP queda sometido al juez ordinario europeo, no a un tribunal propio.
Cooperación Reforzada	Mecanismo (art. 20 TUE + arts. 326-334 TFUE) que permite avanzar a un subconjunto de Estados — al menos 9 — sin unanimidad. Base legal de la EDSPA; el art. 331 TFUE obliga a la Comisión a confirmar la adhesión de quien lo solicite en cuatro meses.
Reforma del Tratado (art. 48 TUE)	Procedimiento de modificación de los Tratados: la Convención se convoca por mayoría simple (el PE ya la activó con la resolución 2022/2051(INL) del 22 de noviembre de 2023), pero la ratificación requiere TODOS los Estados según sus normas constitucionales. Sin unanimidad no hay Tratado.
Viginum	Servicio francés creado en 2021 para vigilar la interferencia informativa extranjera: detecta y publica, no sanciona. Precedente en miniatura del protector puro.

E.4 Términos operativos y técnicos

Término	Definición V3
Doble Verificación humano-IA	Garantía central del sistema (Cap. 8): ningún hallazgo automático se convierte en acto administrativo sin revisión humana. La IA propone; el juicio humano decide e institucionaliza.
Hitos y resultados, nunca procedimientos	Regla de publicación del PP: se publican capacidades, garantías y resultados; nunca modelos, stacks, volúmenes ni metodologías. Aplicada al propio libro en el Anexo B.
Auditoría Algorítmica	Evaluación independiente de sistemas algorítmicos con resultados públicos. El PP audita y remite a los reguladores competentes (DSA, AI Act); no impone sanciones.
Comprobador Ciudadano	Interfaz pública del PP: el ciudadano puede someter un contenido sospechoso y recibir una verificación trazable. La protección visible, no prometida.
Informe Anual de Protección Cognitiva	Publicación anual del PP en las 24 lenguas oficiales: evidencia, resultados del Comprobador, casos verificados y datos abiertos. Base de la rendición de cuentas (Cap. 19).
Paradoja del 60%	La brecha entre la demanda de protección (69% considera la desinformación un problema en su país, Eurobarómetro publicado en febrero de 2026) y la desconfianza hacia el uso gubernamental de la IA (~60%, OCDE 2026). Solo un protector con doble verificación, publicación total y juez independiente puede cerrarla.
Radar Tecnológico	Sistema de vigilancia tecnológica del PP (Cap. 18): interior íntegro, exterior sintético; aceleración de capacidades propia estimada en hasta 3 meses ante brecha detectada.
Alfabetización Cognitiva	Competencia ciudadana para detectar manipulación informativa. Función educativa del PP, al servicio del Decenio Digital 2030 (Decisión (UE) 2022/2481); objetivo del libro: ≥90% de alfabetización en 2038.
IA Resiliente	Sistemas de IA diseñados para resistir ataques, manipulación y fallos manteniendo su funcionalidad y sus garantías.

E.5 Términos económicos y financieros

Término	Definición V3
ROI de la EDSPA	Retorno de la inversión calculado en el Capítulo 9B: 164% a cinco años, con +€1.820M/año de beneficio neto estimado.
Inversión EDSPA	€1.100M de inversión inicial, con 3.000 empleos directos en 2035 y 6.000-9.000 indirectos; impacto PIB €3.160M-4.000M (Cap. 9B).
Dotación del Poder Protector	Dotación financiera estable del PP una vez constitucionalizado: €2.600M en dotación inicial, hasta €3.400M a madurez (Cap. 17). Más de 15.000 empleados directos en madurez 2040+ y un ecosistema de 55.000-68.000 empleos (Cap. 17).
Recursos propios (art. 311 TFUE)	Vía de financiación autónoma de la UE (sistema vigente: Decisión (UE, Euratom) 2020/2053) que el libro propone explorar para la dotación del PP: quien depende del presupuesto anual de otros no es un poder.

E.6 Términos geopolíticos

Término	Definición V3
Big Tech	Grandes plataformas tecnológicas que dominan la infraestructura de la esfera cognitiva. Actores regulados por el acervo europeo (DSA, DMA, AI Act), no adversarios existenciales del libro.
Los Dos Centenarios	Objetivos declarados por China para 2021 (sociedad moderadamente próspera) y 2049 (centenario de la República Popular: país socialista moderno). El espejo temporal del libro: 2049, no 2039.
China Standards 2035	Estrategia de estandarización tecnológica china. Ejemplo del método del rival: las profecías con fecha son su herramienta, no la del libro.
Soft Power	Capacidad de influir por atracción (valores, cultura, resultados) y no por coerción. La proyección internacional del PP funciona por efecto Bruselas: se copia lo que funciona.
Tres modelos en competencia	La taxonomía del Cap. 21: modelo de mercado (EE. UU.), modelo de control (China) y modelo democrático europeo. Cada uno con fortalezas y debilidades; solo el europeo puede a la vez monetizar y proteger la atención, y solo con ejecutor.

E.7 Marco normativo (referencias exactas)

Término	Referencia V3
DSA	Reglamento (UE) 2022/2065 sobre el Mercado Único de Servicios Digitales. Obligaciones de plataformas; arts. 37 (auditorías anuales independientes, primera ronda ago-2024) y 40 (acto delegado, julio 2025, acceso de datos para investigadores).
AI Act	Reglamento (UE) 2024/1689. Normas armonizadas sobre inteligencia artificial.
RGPD	Reglamento (UE) 2016/679. Protección de datos personales; art. 25 (privacidad por diseño).
Data Act	Reglamento (UE) 2023/2854. Acceso y compartición de datos.
Decenio Digital 2030	Decisión (UE) 2022/2481: 20M especialistas TIC, 80% de competencias básicas 16-74, 75% de empresas con cloud/IA.
Escudo Europeo de la Democracia	Comunicación de la Comisión de 12 de noviembre de 2025 contra la interferencia extranjera.
Carta de los Derechos Fundamentales	Arts. 7, 8, 11 (privacidad, datos, información) y 47 (tutela judicial efectiva): la garantía jurisdiccional del sistema.
Convenio Marco del Consejo de Europa sobre IA	Primer tratado vinculante mundial sobre IA, abierto a firma el 5 de septiembre de 2024 en Vilna; firmado por la Comisión en nombre de la UE.
Principios Globales ONU para la Integridad de la Información	Presentados por el Secretario General el 24 de junio de 2024; derivados de «Nuestra Agenda Común» (2021).

E.8 Las fechas del libro (corregidas)

Año	Hito V3
2027-2030	EDSPA: agencia de transición por cooperación reforzada, 9 Estados fundadores.
~2030	Convención sobre la reforma de los Tratados (activable por mayoría simple; el PE ya votó activar el art. 48(2) TUE en 2023).
2031-2032	Firma del Tratado que institucionaliza el Poder Protector.
2033	Entrada en vigor del Poder Protector como 4º poder constitucional.
2033-2035	Integración de la EDSPA en el PP.
2038	Objetivo de alfabetización cognitiva ≥90% (función educativa del PP).
2040+	Madurez del PP: >15.000 empleados directos, ecosistema 55.000-68.000 empleos.
2049	Espejo del libro: centenario de la República Popular China. Se usa una sola vez, como elección entre modelos terminados, no como profecía.

E.9 Acrónimos

Acrónimo	Significado
UE	Unión Europea
TUE / TFUE	Tratado de la Unión Europea / Tratado de Funcionamiento de la UE (DOUE C 326, 2012)
EDSPA	European Digital Sphere Protection Agency
PP	Poder Protector
DSA / DMA	Digital Services Act (2022/2065) / Digital Markets Act
RGPD	Reglamento General de Protección de Datos (2016/679)
FIMI	Foreign Information Manipulation and Interference (SEAE)
ENISA	Agencia de la UE para la Ciberseguridad
EDMO	European Digital Media Observatory (hubs hasta 2026)
SEAE	Servicio Europeo de Acción Exterior
TJUE	Tribunal de Justicia de la Unión Europea
NIST	National Institute of Standards and Technology (EE. UU.): AI RMF 1.0 (2023), perfil IA generativa AI 600-1 (2024)
ISO/IEC 42001:2023	Primer estándar de sistema de gestión de IA certifiable
ANSSI / NCSC	Agencia francesa de ciberseguridad (2009) / National Cyber Security Centre británico (2016): precedentes institucionales
OCDE / ONU / CoE	Organización para la Cooperación y el Desarrollo Económicos / Organización de las Naciones Unidas / Consejo de Europa

E.10 Términos por parte del libro (estructura V3, 21 capítulos)

Parte I — Diagnóstico (Capítulos 1-5)

Esfera cognitiva digital · Desinformación (mis/dis/malinformation) · Deepfake · Manipulación algorítmica · Vulnerabilidad democrática · Brecha de soberanía.

Parte II — El Parche (Capítulos 6-10, incluido el nuevo 9B)

EDSPA · Cooperación reforzada · Base legal (arts. 114, 16, 352 TFUE; 20 TUE + 326-334 TFUE) · 9 Estados fundadores · ROI 164% · Doble verificación.

Parte III — La Solución Definitiva (Capítulos 11-20)

Transición EDSPA→PP · Arquitectura institucional (Sala de Recurso, Cámara Especializada, casación TJUE) · Competencias · Financiación (art. 311 TFUE) · Ecosistema 55.000-68.000 empleos · Radar tecnológico · Paradoja del 60% · Informe Anual de Protección Cognitiva · Camino art. 48 TUE.

Parte IV — La Visión Final (Capítulo 21)

Tres modelos en competencia · Efecto Bruselas · Espejo 2049.

Anexo E — Glosario V3 | Poder Protector: La Protección Cognitiva como el 4º Poder Constitucional de Europa

Adrian Potentela | 25 de septiembre de 2026

Anexo F: Divisiones de Especialización Operativa

Por qué este anexo existe y por qué es un anexo

Los capítulos 12 y 13 fijan la arquitectura institucional y los límites constitucionales del Poder Protector; el Anexo B fija sus capacidades. Este anexo describe la dimensión que ambos dejan implícita: **la especialización operativa**. La esfera cognitiva no es un dominio homogéneo — la manipulación que viaja en un anuncio programático no se detecta, audita ni educa como la que viaja en una red de bots, ni como la que está embebida en el diseño de un banner de consentimiento. Una institución que pretenda proteger toda la esfera con una sola caja de herramientas protegerá mal cada parte de ella. La especialización no es un lujo organizativo del PP: es una **función casi intrínseca**, tan consustancial a su misión como la propia doble verificación.

Es anexo — y no capítulo — por la misma doctrina que gobierna todo el libro: las divisiones son **materia operativa**. La constitución del PP (Caps. 12-15) fija poderes, límites, financiación y trayectoria; el organigrama operativo que la sirve puede — y debe — evolucionar por disparadores de madurez, no por reforma constitucional. Donde un cambio de capítulo exigiría una Convención, un cambio de división exige solo el reglamento interno y la rendición de cuentas anual ante el Parlamento Europeo (Cap. 19).

F.1 La doctrina: capacidades específicas, límites universales

Todo lo que este anexo dice hereda sin excepción la regla del Anexo B: se publican **capacidades, garantías y taxonomías; nunca procedimientos ni técnicas**. Y añade una regla propia, que gobierna cada división sin excepción:

La especialización divide el trabajo; nunca divide los límites. Cada división del PP dispone de su propia IA forense y de sus propios operadores especializados, pero las cinco funciones del Capítulo 13 — detectar, auditar, publicar, remitir, educar — y sus límites (no sanción, no filtro, no etiquetas de verdad, simetría anti-arma) son **idénticos en todas**. No existe una división «dura» y una división «blanda»: existe una sola doctrina aplicada a dominios distintos de la amenaza.

Esta arquitectura responde además a una objeción previsible: la especialización podría parecer el primer paso hacia una agencia de seguridad con competencias por dominio. El diseño la impide por construcción. Cada división produce los mismos tres artefactos públicos del Anexo B (informe, evidencia reproducible, expediente de remisión), transfiere sus expedientes a los mismos sancionadores (Comisión y autoridades nacionales: DSA 6%, AI Act 7%, RGPD) y opera bajo el mismo protocolo transversal de doble verificación humano-IA del Capítulo 8 (IA propone, humano decide; escalado a segundo analista en discordancia Alto/Crítico). **Cambiar el dominio no cambia la naturaleza del poder.**

F.2 El principio de diseño modular: la plantilla de división

Cada división es una instanciación de una misma plantilla con cinco componentes fijos:

Componente	Qué es	Referencia
IA forense específica	Un sistema de detección entrenado para el patrón de manipulación de su dominio; abierta, auditable y explicable	Cap. 18 (IA propia); Anexo B (capacidades, no técnicas); F.7 (auditoría de las propias IAs)
Operadores especializados	Personal con el perfil profesional del dominio (véase F.4); el juicio humano firma siempre	Cap. 8 (doble verificación); Cap. 17 (contrapeso IA: el mayor empleador público del juicio humano no automatizable)
Protocolo transversal	Detección IA → verificación humana → escalado en discordancia Alto/Crítico → publicación o remisión	Cap. 8, obligatorio y con trazabilidad auditable
Acervo que ejecuta	Ninguna división crea derecho nuevo: cada una hace sistemático y verificable un acervo existente	Cap. 13 (DSA, AI Act, RGPD/ePrivacy, Data Act, Escudo Europeo de la Democracia, EU KIDS Act)
Interfaz pública	Salida por el portal de evidencia y las métricas públicas; ninguna división tiene canal propio ni secreto	Anexo B (B.6); Cap. 19 (transparencia por defecto)

La modularidad tiene una consecuencia estratégica: **añadir una división nueva no toca la constitución del PP**. Cuando en 2040+ emerja un dominio hoy inexistente (interfaces cerebro-máquina, agentes IA autónomos de persuasión a escala individual), la respuesta institucional será un reglamento interno y una línea de plantilla — no una Convención. La especialización es, también, la cláusula de futuro del Poder Protector.

F.3 El mapa de divisiones

División	Dominio de amenaza	Capacidad nuclear	Acervo que hace sistemático	Qué nunca hace
F.3.1 Adtech	Manipulación monetizada: desinformación con ánimo de lucro, publicidad política opaca, microsegmentación explotadora	Auditoría forense de la cadena publicitaria y del archivo de anuncios; evidencia de quién paga, qué segmenta y con qué datos	DSA arts. 39 (publicidad política) y 26-28 (publicidad y recomendaciones); RGPD art. 22	No prohíbe anuncios; no fija tarifas; publica y remite
F.3.2 Actores Sintéticos	Bots, granjas de trolls, amplificación coordinada, FIMI, deepfakes de identidad (véase la sección dedicada más abajo)	Cuantificación pública de la actividad sintética en conversaciones públicas: proporción, coordinación y origen de la amplificación artificial; exposición con pruebas de imitaciones digitales de personas identificables	AI Act art. 50 (transparencia de IA); clasificación FIMI del SEAE; DSA arts. 35 y 34 (deepfakes); ley danesa de imagen (véase abajo)	No retira cuentas (plataformas/autoridades); no etiqueta contenido individual: publica patrones agregados; no rastrea a las personas
F.3.3 Arquitectura Cognitiva	Dark patterns, fricción del consentimiento, diseño de la adicción y de la ira	Auditoría del diseño: índice público de fricción del consentimiento y de arquitecturas de manipulación por plataforma	DSA art. 25 (dark patterns prohibidos); RGPD art. 25 (privacidad desde el diseño); ePrivacy; Digital Fairness Act (en tramitación)	No rediseña plataformas; rankea <i>diseños</i> , jamás contenidos ni discurso
F.3.4 Electoral	Interferencia electoral, opacidad de campaña, operaciones FIMI de ciclo corto	Monitoreo de campañas y archivo verificable de publicidad política; activación del protocolo electoral de la EDSPA	DSA arts. 36-39; Rapid Response System 2024 (EDMO); Escudo Europeo de la Democracia (nov-2025)	No certifica resultados; no silencia campañas: publica evidencia para electores y autoridades
F.3.5 Menores	Diseño adictivo infantil, rutas de acceso por edad frágiles, exposición a manipulación; el embrión de depredación (grooming) como arquitectura facilitada	Auditoría de cumplimiento infantil por plataforma (EU KIDS Act), índice público de diseño seguro para menores y materiales de alfabetización temprana	EU KIDS Act (COM(2026) 681, sep-2026); DSA arts. 28-30 y guías de protección de menores (jul-2025); RGPD arts. 8 y 25; blueprint europeo de verificación de edad; Cyberbullying Action Plan; Digital Fairness Act (en tramitación)	No vigila a menores ni conversaciones privadas (materia penal: Estados/Europol); no filtra contenidos (plataformas/padres/Estados): audita diseño y cumplimiento, y remite patrones agregados

F.3.6 Plataformas Conversacionales	Agentes de IA en el debate público sin identificación, sesgo sistemático de modelos, persuasión sintética	Contraste de cumplimiento de transparencia art. 50 AI Act y auditoría de sesgos declarados	AI Act arts. 50 y 6; DSA art. 35	No «aprueba modelos»; no sanciona su despliegue: publica y remite
F.3.7 Métricas Públicas	Opacidad estructural: la imposibilidad de comparar plataformas y períodos	La función de publicación transversal: informe anual, etiqueta nutricional digital, series comparables por plataforma y Estado	Reglamento 1049/2001; art. 15(3) TFUE; art. 42 Carta	No interpreta: mide, agrega y publica con metodología abierta

F.3.2.bis Identidad digital sintética: el patrón y la prueba

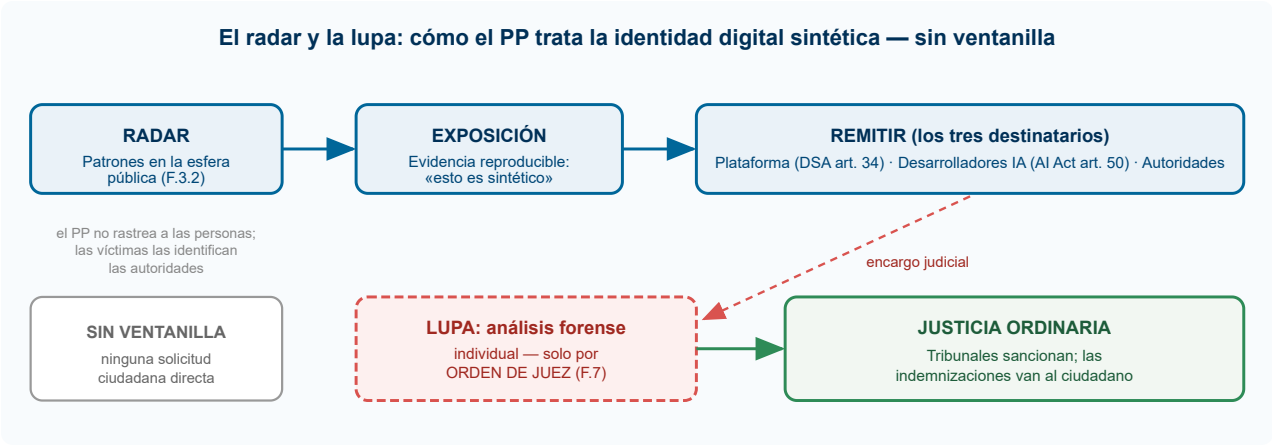
Un caso de uso concentra todas las líneas rojas del PP y merece sección propia: la detección de imitaciones digitales realistas de personas identificables — deepfakes de rostro, voz o cuerpo — en circulación pública. El anclaje legal ya existe: **Dinamarca** fue el primer Estado de la UE en reconocer a cada persona derechos de propiedad intelectual sobre su propia imagen, voz y cuerpo (reforma de la Ophavsretsloven, en vigor el 1 de julio de 2026), su presidencia del Consejo de la UE aboga por extender el modelo a toda Europa, y el DSA (art. 34) y el AI Act (art. 50) ya obligan a plataformas y desplegados a la transparencia sobre contenido sintético. La precisión importa: la ley danesa otorga un **derecho** al ciudadano; no crea ningún registro biometric estatal — es el titular quien se autentica ante su autoridad.

Sobre ese acervo, el flujo del PP es estrictamente el de sus cinco funciones — ninguna nueva:

1. **Detectar el patrón:** la IA forense de la división identifica imitaciones digitales de personas identificables y su circulación en la esfera pública, bajo doble verificación humano-IA (Cap. 8).
2. **Publicar las pruebas:** exposición con evidencia reproducible en el portal público — «este contenido es sintético; estas son las pruebas».
3. **Remitir a los tres destinatarios naturales:** la **plataforma** que lo aloja (obligaciones DSA/AI Act), los **desarrolladores de IA implicados** (trazabilidad del modelo generador, AI Act art. 50) y las **autoridades competentes**.

Y una cosa que el PP deliberadamente **no** hace: **avisar al ciudadano perjudicado**. La identificación de las personas afectadas y su notificación corresponden a las autoridades — que tienen el mandato, los datos y la legalidad para hacerlo. El PP no conoce a las víctimas ni necesita conocerlas: *expone la manipulación; no rastrea a las personas*.

Por qué no hay ventanilla ciudadana. Un servicio que recibiera solicitudes directas sería un objetivo de colapso: cualquier actor hostil podría generar millones de solicitudes falsas para saturar al PP y proclamar su fracaso. El diseño lo excluye por construcción — el caso individual solo alcanza al PP por dos vías: emerge del monitoreo de patrones públicos, o llega como **encargo judicial** (véase el Departamento Pericial Judicial, F.7). No existe el buzón por el que llegaría la avalancha.



El resultado de este diseño es una división que protege el derecho emergente del ciudadano europeo sobre su identidad digital sin convertirse nunca en agencia de identificación: un solo estándar probatorio técnico para Europa, y tantas puertas legales como Estados — hasta que la convergencia que la presidencia danesa persigue haga el resto.

F.4 Operadores: el perfil humano de cada división

La especialización de las IAs sería hueca sin su contrapartida humana. Cada división recluta perfiles que hoy existen dispersos en el mercado laboral europeo y que el PP agrega en una carrera pública nueva — el empleo cualificado del ecosistema del Cap. 17:

División	Perfiles operadores (existente hoy en el mercado)
Adtech	Audidores de programática, especialistas en fraude publicitario, economistas del adtech, juristas de publicidad y consumo
Actores Sintéticos	Analistas OSINT, lingüistas forenses (estilometría), analistas de grafos de redes, expertos FIMI (perfil SEAE/Viginum), peritos forenses de medios sintéticos
Arquitectura Cognitiva	Psicólogos cognitivos, especialistas UX de auditoría, juristas RGPD/ePrivacy, científicos del comportamiento
Electoral	Politólogos, expertos en sistemas electorales, analistas por Estado miembro, juristas electorales
Menores	Psicólogos evolutivos, pediatras de conducta, mediadores digitales, educadores, auditores de diseño seguro infantil
Plataformas Conversacionales	Especialistas en LLM, auditores algorítmicos, juristas AI Act, «red teamers» de persuasión sintética
Métricas Públicas	Científicos de datos, periodistas de datos, estadísticos, especialistas en comunicación (Cap. 19)

Tres observaciones de diseño. Primera: los perfiles más escasos (auditores algorítmicos, lingüistas forenses) son precisamente los que el PP tendría que formar internamente — una función adicional de la división de Educación Cognitiva del Cap. 12. Segunda: cada división alimenta la paradoja del 60% (Cap. 19) con su respuesta de diseño: cuanta más IA específica, más juicio humano firma — el contrapeso IA del Cap. 17 escala con la especialización, no contra ella. Tercera: la doble afiliación es la regla — cada operador pertenece a una división y al protocolo transversal del Cap. 8, de modo que el intercambio de analistas entre divisiones es una capacidad institucional (trazable), no una excepción.

F.5 Activación por etapas: la especialización sigue la dotación

Las divisiones no nacen todas a la vez: se activan por los mismos disparadores de madurez que gobiernan la trayectoria de dotación de personal de los Capítulos 15 y 17. Este anexo no fija fechas de división — fija el orden y la condición:

Etapa	Plantilla del PP	Divisiones activas	Condición de activación
EDSPA (2027-2030)	1.500-2.000	Embrión: Electoral + Actores Sintéticos (mandato de la agencia, Cap. 8) + componente de auditoría de diseño infantil de Menores (verificación del EU KIDS Act, COM(2026) 681; aplicación prevista desde 2027 una vez adoptado)	Mandato de la EDSPA (Cap. 8): protección electoral y monitoreo de actividad sintética
Núcleo (2033-2035)	~3.000	+ Adtech, + Métricas Públicas; Menores amplía a alfabetización temprana	Informe de impacto 2030-2031 favorable; reglamento interno del PP
Pleno (~2037)	~7.000-8.000	+ Arquitectura Cognitiva, + Plataformas Conversacionales; Menores a capacidad casi plena	27 Estados / 24 lenguas / 24-7 operativos (disparadores del Cap. 15)
Madurez (2040+)	>15.000	+ Menores a plena capacidad; nuevas divisiones por dominios emergentes	Evaluación bienal ante el PE; solo si es favorable

Nota de rigor: la columna de plantilla es la trayectoria consensuada de dotación (Caps. 12, 15, 17), no una previsión de contratación por división. El reparto interno de plantilla entre divisiones es materia del reglamento interno y del Informe Anual — publicable como resultado, no presupuestable por anticipado en un anexo. La excepción deliberada es el componente de auditoría de diseño infantil de Menores en el embrión: su justificación no es organizativa sino de demanda — el EU KIDS Act (propuesta COM(2026) 681, sep-2026) exige verificación sistemática de diseño seguro exactamente en la ventana en que la EDSPA arranca.

F.6 Coherencia presupuestaria y de garantías

Dos cierres para que este anexo no desalineee la economía del libro. Primero, **presupuesto**: las divisiones son subunidades de los cuatro departamentos del Capítulo 12 (Protección Cognitiva, Soberanía Digital, Educación Cognitiva, Inteligencia Cognitiva) dentro de sus techos de etapa plena (€1.000M/500M/300M/200M) y del marco del Cap. 17 — ninguna división tiene presupuesto propio ni línea nueva. El ejemplo de correspondencia más natural: Adtech, Actores Sintéticos, Arquitectura Cognitiva, Electoral, Menores y Plataformas Conversacionales dependen de Protección Cognitiva; Métricas Públicas comparte interfaz con Inteligencia Cognitiva — su función es de publicación transversal (interfaz), no de operación de campo, y el techo de Inteligencia basta. Segundo, **garantías**: cada división hereda íntegro el bloque B.5 del Anexo B — doble verificación no automatizable, transparencia por defecto, privacidad desde el diseño, simetría anti-arma y separación estricta entre detectar y sancionar. La Sala de Recurso administrativa y la Cámara Especializada en Protección Digital del Tribunal General (Cap. 12) son la vía de recurso frente a cualquier actuación de *cualquier* división.

F.7 La auditoría de los auditores: el meta-nivel de la especialización

La especialización plantea una última pregunta, la que cualquier escéptico informado formulará: *¿quién audita a las IAs especializadas y a los técnicos que las entrenan, las operan y las certifican?* Si cada división dispone de su propia IA forense, el sistema descansa sobre modelos que nadie fuera del PP puede ver. La respuesta del diseño es institucional: el PP audita sus propios sistemas con la misma doctrina con la que audita la esfera — **la luz empieza por casa**.

Tres piezas. **Primera: trazabilidad del entrenamiento**. Cada modelo de división mantiene un registro auditable de sus datos de entrenamiento, versiones, rendimiento y deriva — el mismo estándar de trazabilidad que el Cap. 8 exige a las plataformas que el PP audita. **Segunda: formación interna de los perfiles escasos**. Los auditores algorítmicos y lingüistas forenses que el sistema necesita apenas existen hoy en el mercado laboral europeo (F.4); el PP los forma internamente vía Educación Cognitiva, y esa carrera pública incluye la certificación de los propios auditores — quién puede auditar una IA de división es información pública. **Tercera: la doble verificación aplicada hacia dentro**. El protocolo del Cap. 8 rige también para los sistemas propios del PP: ningún hallazgo producido por una IA de división se publica o remite sin firma humana, y el PP permanece como el mayor empleador público europeo del juicio humano también sobre sus propios modelos — el contrapeso IA del Cap. 17, aplicado al interior.

El Departamento Pericial Judicial — la «lupa» del flujo de identidad digital (F.3.2.bis) — ancla aquí como **subunidad de Inteligencia Cognitiva**: soporte técnico transversal al servicio de la cooperación judicial, sin quinto departamento y sin línea presupuestaria nueva (dentro del techo de €200M de Inteligencia, Cap. 12). Sus reglas son estrictas: **solo un juez** — el único órgano con garantía procesal (partes, defensa, contradicción) — puede solicitar

un análisis forense individual de la esfera digital de una persona; ninguna autoridad administrativa ni particular accede al canal. Cada solicitud se registra con juez titular, número de procedimiento, jurisdicción y objeto del análisis (archivo operativo protegido del Cap. 7); cada análisis, con operador firmante, doble verificación, IA de división utilizada y datos accedidos — todo consultable por el tribunal y los órganos de garantía (Sala de Recurso modelo ACER, Cámara Especializada del Cap. 12). El radar no se convierte en lupa salvo por orden judicial; y la lupa solo mira lo que el encargo judicial fija. Si algo se sale del objeto del encargo, la trazabilidad lo muestra.

Lo que este anexo deliberadamente no hace: no crea competencias nuevas ni diluye las cinco funciones del Capítulo 13 — las multiplica por dominio bajo el mismo límite constitucional. No publica arquitecturas, modelos, umbrales ni metodologías de ninguna IA de división (regla B.1) — la auditoría de F.7 se publica como garantía y capacidad, nunca como técnica. Y no convierte la especialización en burocracia: si una división no produce artefactos públicos verificables, el Informe Anual debe poder decirlo — la luz empieza por casa.