LA INTELIGENCIA ARTIFICIAL EN LA SOMBRA EN EL SECTOR LEGAL

Riesgos de confidencialidad, secreto profesional y estrategias de compliance ante el uso no autorizado de transcripción automática en reuniones con clientes

Firma Scarpa / Ricardo Scarpa

Junio de 2026

derechoartificial.com

DERECHO ARTIFICIAL

Índice

Resumen ejecutivo

El fenómeno del *Shadow AI* o inteligencia artificial en la sombra —uso no autorizado de herramientas de IA por profesionales que eluden los controles institucionales— se ha consolidado como un riesgo crítico en el sector legal. Este artículo analiza específicamente el empleo clandestino de asistentes de notas y sistemas de transcripción automática en reuniones con clientes, y sus consecuencias directas sobre el secreto profesional, la confidencialidad y el cumplimiento normativo. Mediante una metodología cualitativa basada en el análisis de normativa europea y española (RGPD, AI Act, LOPDGDD, Circulares del CGAE), jurisprudencia reciente, resoluciones de autoridades de control y literatura técnica especializada, se demuestra que el *Shadow AI* provoca una "erosión del aseguramiento" irreversible al transferir datos de voz de clientes a nubes opacas sin garantías contractuales. El artículo identifica infracciones sistémicas al principio de exactitud, transparencia y responsabilidad proactiva del RGPD, así como vulneraciones directas del deber de supervisión humana exigido por el Reglamento (UE) 2024/1689. Se sistematizan casos de sanciones por "alucinaciones" y pérdida del privilegio abogado-cliente (2024-2026), y se analiza el endurecimiento de las coberturas aseguradoras frente a la IA no auditada. Finalmente, se propone una hoja de ruta de cuatro fases —descubrimiento activo, homologación de entornos, transparencia reforzada y verificación humana documentada— que transforma el cumplimiento normativo en una ventaja competitiva basada en la soberanía operativa sobre el dato del cliente.

Palabras clave: *Shadow AI*, secreto profesional, transcripción automática, asistentes de notas, RGPD, AI Act, responsabilidad profesional, cumplimiento normativo, abogacía.

1. Introducción

1.1. Contexto: La consolidación estructural de la inteligencia artificial en la abogacía

El ejercicio del derecho se halla inmerso en una transformación sin precedentes, marcada por la transición de una fase de experimentación tecnológica a una de adopción estructural de la inteligencia artificial (IA). Según los hallazgos del informe *Future Ready Lawyer 2026* —estudio de alcance global con más de 2.500 encuestados en 12 países—, el 92% de los juristas a nivel global ya integra al menos una herramienta de IA en su flujo de trabajo diario [1]. Esa integración no es periférica: alcanza el núcleo de la práctica jurídica en tareas de investigación legal, redacción de borradores y revisión de documentos complejos . El motor de este despliegue masivo es una promesa de eficiencia disruptiva, con ahorros de tiempo semanales reportados de entre el 6% y el 20%, lo que ha comenzado a cuestionar la viabilidad a largo plazo del modelo tradicional de la hora facturable [2].

Sin embargo, esa celeridad en la adopción ha generado una brecha de gobernanza crítica. Mientras los departamentos de tecnologías de la información (TI) y cumplimiento normativo intentan diseñar marcos de uso seguro, la presión por la productividad y la facilidad de acceso a herramientas de IA de frontera —gratuitas o de bajo coste— han propiciado el fenómeno del *Shadow AI* o "IA en la sombra" [2]. Se define este fenómeno como el uso informal, *ad hoc* y no autorizado de sistemas de IA por parte de los profesionales para realizar tareas laborales, eludiendo los canales de supervisión y las políticas de seguridad de la firma [3]. En el sector legal, este uso clandestino se manifiesta de forma especialmente aguda en el empleo de asistentes de notas y bots de transcripción automática en reuniones con clientes .

1.2. Justificación: El riesgo de la "erosión del aseguramiento"

La gravedad del *Shadow AI* en los despachos de abogados no reside únicamente en la elusión de la política interna, sino en lo que la literatura técnica reciente denomina la "erosión del aseguramiento" (*assurance erosion*) [3]. En un entorno donde la confidencialidad y el secreto profesional son piedras angulares de la confianza y el derecho de defensa, la introducción de datos de clientes en sistemas en la nube no auditados representa una amenaza sistémica [2]. Herramientas populares de transcripción automática, a menudo integradas de forma pasiva en plataformas de videoconferencia, capturan flujos de datos de voz que son procesados en servidores de terceros cuyos términos de servicio suelen autorizar el uso de la información de entrada para el reentrenamiento de modelos comerciales [4].

Este tratamiento de datos personales de voz —que por su naturaleza permiten identificar o hacer identificable a una persona física [4]— se produce frecuentemente sin una base jurídica clara, sin evaluaciones de impacto en protección de datos (EIPD) previas y vulnerando el principio de transparencia activa . La Agencia Española de Protección de Datos (AEPD) ha subrayado que una firma jurídica asume plenamente la condición de responsable del tratamiento al emplear estas herramientas, debiendo ejercer una diligencia debida que no constituye un trámite formal único, sino un deber de supervisión continuo durante todo el ciclo de vida del sistema . El uso no autorizado de estos transcriptores rompe de inmediato el privilegio abogado-cliente, asimilando la práctica al acto negligente de abandonar expedientes confidenciales en un espacio público [2].

1.3. Pregunta de investigación y objetivos

Ante este escenario, el presente artículo académico-profesional aborda la siguiente pregunta de investigación: ¿Cómo afecta el fenómeno del *Shadow AI*, específicamente a través del uso de herramientas de transcripción automática no autorizadas, a los deberes deontológicos de secreto profesional y confidencialidad en la abogacía contemporánea, y qué marcos de gobernanza proactiva permiten mitigar estos riesgos bajo el Reglamento (UE) 2024/1689 (AI Act)?

Para dar respuesta a esta interrogante, se formulan los siguientes objetivos operativos:

1. Analizar el alcance técnico y jurídico del fenómeno del *Shadow AI* en los despachos de abogados, diferenciando entre el uso de IA autorizada y las integraciones no declaradas de herramientas de transcripción [3].

2. Examinar el impacto deontológico en el secreto profesional y el privilegio abogado-cliente, contrastando la doctrina ética de la American Bar Association (ABA) con las recientes Circulares del Consejo General de la Abogacía Española (CGAE), en especial la Circular 3/2026 [2,5].

3. Identificar el régimen sancionador y las infracciones bajo el Reglamento General de Protección de Datos (RGPD) y la LOPDGDD derivadas de la transcripción de voz sin garantías [4].

4. Evaluar la aplicación del Reglamento (UE) 2024/1689 en el entorno de las firmas jurídicas, clasificando los niveles de riesgo y las obligaciones de supervisión humana [5].

5. Proponer una hoja de ruta de cumplimiento y gobernanza preventiva que sustituya la prohibición genérica por una soberanía operativa real y auditable [23].

1.4. Metodología

La elaboración de este estudio se basa en una metodología cualitativa y analítica de carácter multidisciplinar. Se ha procedido, en primer término, a una revisión exhaustiva de la literatura técnico-jurídica y académica publicada entre 2024 y el primer semestre de 2026, incluyendo repositorios científicos como arXiv para conceptualizar la arquitectura de gobernanza de la IA [3]. Dichos preprints han sido contrastados con fuentes normativas y doctrinales revisadas por pares para garantizar la solidez de los argumentos. En segundo lugar, se analizan fuentes normativas y jurisprudenciales de primer orden, con especial atención al marco europeo (RGPD, AI Act) y español (Ley Orgánica del Derecho de Defensa) [2,4].

El análisis incorpora asimismo los resultados de encuestas sectoriales de alto nivel, como el estudio *Future Ready Lawyer*, para cuantificar la prevalencia del fenómeno [1]. Desde el punto de vista deontológico, se contrastan las guías de buenas prácticas emitidas por colegios de abogados de referencia, como el Ilustre Colegio de la Abogacía de Madrid (ICAM) y el CGAE, a través de su *Libro Blanco sobre Inteligencia Artificial y Abogacía* [2,5]. Finalmente, se emplea el método del caso para examinar resoluciones administrativas de autoridades de control, como la AEPD, y sentencias recientes sobre responsabilidad profesional derivada de "alucinaciones" o errores algorítmicos [4].

El enfoque adoptado es el de "IA por diseño" (*AI by design*), reconociendo que la tecnología opera como un colaborador infraestructural indispensable que exige, sin embargo, una reserva de humanidad y un juicio profesional reforzado [5,6]. La respuesta del *compliance* no es el bloqueo tecnológico, sino la articulación de sistemas de observabilidad y telemetría que garanticen que ningún dato de cliente cruza la frontera de la firma sin una validación explícita [3]. En este sentido, el deber de responsabilidad proactiva del artículo 5.2 del RGPD obliga al despacho a demostrar, no solo a declarar, que la confidencialidad se mantiene en cada fase del tratamiento [4].

2. Definición y alcance del Shadow AI en el entorno jurídico

2.1. Conceptualización: De la tecnología en la sombra a la IA en la sombra

Para comprender el desafío que representa el uso no supervisado de asistentes de notas, resulta necesario definir el fenómeno del *Shadow AI* (inteligencia artificial en la sombra). Dicho fenómeno constituye una evolución disruptiva del tradicional *Shadow IT*, término acuñado hace más de una década para describir el uso de servicios en la nube (como Dropbox o Google Drive) fuera del control del departamento de sistemas [2,3,8]. La literatura técnica del primer semestre de 2026 advierte, no obstante, que el *Shadow AI* presenta características únicas que lo hacen sustancialmente más peligroso que su predecesor [7].

Mientras que el *Shadow IT* implicaba la instalación de software o hardware no autorizado, el *Shadow AI* opera fundamentalmente en la "capa de interacción" [7,9]. Ello significa que no requiere instalaciones complejas; basta con un navegador o una aplicación móvil para que un abogado introduzca flujos de datos confidenciales en motores de IA de frontera [3]. Procede definir, por tanto, el *Shadow AI* en el entorno jurídico como el uso informal, *ad hoc* y no autorizado de herramientas de IA generativa por parte de los profesionales para realizar tareas laborales —como transcribir reuniones o redactar borradores—, eludiendo activamente los canales de supervisión, seguridad y cumplimiento de la firma [2].

2.2. Diferencias críticas entre IA autorizada e IA en la sombra

La distinción entre un sistema de IA institucional y uno "en la sombra" no es meramente administrativa, sino que reside en la integridad de la frontera de aseguramiento (*assurance boundary*) del despacho [3,7]. El análisis revela tres diferencias fundamentales:

Primera diferencia: gobernanza de datos y reentrenamiento. Las herramientas autorizadas (modalidades *Enterprise*) suelen contar con cláusulas de "no-reutilización", garantizando que los datos de los clientes no se utilicen para entrenar modelos comerciales del proveedor [2,5]. En cambio, las versiones gratuitas o de consumo que caracterizan al *Shadow AI* suelen autorizar en sus términos de servicio el uso de los *prompts* y audios para el refinamiento de sus algoritmos, lo que supone una filtración permanente de la propiedad intelectual y el secreto profesional [10].

Segunda diferencia: transparencia y explicabilidad. Los sistemas aprobados por la firma deben pasar por un proceso de homologación que verifique su trazabilidad [5,6]. El *Shadow AI* es inherentemente opaco: el departamento de

compliance no puede ver qué herramientas se están utilizando ni qué datos están cruzando el perímetro del despacho [7,9].

Tercera diferencia: seguridad y ciberseguridad. Las herramientas no autorizadas introducen dependencias de terceros no documentadas [3]. Mientras que las herramientas oficiales se integran en el inventario de activos digitales del despacho bajo el Esquema Nacional de Seguridad (ENS), la norma ISO 42001 de gestión de sistemas de IA o estándares equivalentes, el *Shadow AI* expande la superficie de ataque de la firma sin que esta tenga conciencia de ello [2,7,11].

2.3. Prevalencia del fenómeno: Una realidad omnipresente

Los datos analizados indican que el *Shadow AI* no es una práctica marginal, sino una condición sistémica de la abogacía contemporánea. Según el informe *Future Ready Lawyer 2026*, si bien el 92% de los juristas utiliza IA, existe una brecha crítica de percepción: mientras que el 81% de los despachos cree que la regulación de la IA tendrá un gran impacto, solo el 34% se siente realmente preparado para gestionarla [1]. Esta falta de preparación proactiva constituye el caldo de cultivo ideal para el uso clandestino de herramientas .

Estudios empíricos recientes realizados en organizaciones de infraestructuras críticas —extrapolables al sector legal en lo que respecta a la dinámica de gobernanza, con las necesarias cautelas sectoriales— muestran que el uso de IA en la sombra es "omnipresente" [3]. En encuestas de 2026, los responsables de seguridad informan que el uso de herramientas de IA de frontera (como ChatGPT, Claude o Gemini) suele preceder por meses a la implementación de políticas internas . Un hallazgo especialmente revelador es que, incluso tras la adopción de herramientas oficiales (como Microsoft Copilot), el uso de *Shadow AI* persiste debido a la percepción de que las herramientas públicas son "más capaces" o "menos restrictivas" . En el sector jurídico, esto se traduce en abogados que, por razones de inmediatez, prefieren usar un transcriptor gratuito en su dispositivo personal durante una reunión con un cliente antes que aguardar a la validación de la herramienta corporativa [2].

2.4. Factores impulsores: ¿Por qué los abogados eluden el control?

La emergencia del *Shadow AI* en los despachos no responde a una intención maliciosa, sino a una serie de factores estructurales y culturales bien identificados en la literatura:

Primero, la presión por la productividad y el ahorro de tiempo: con ahorros reportados de hasta el 20% semanal, los abogados perciben la IA como una vía de supervivencia ante la carga de trabajo [12]. El 62% de los juristas ya prioriza la eficiencia sobre los métodos tradicionales . Segundo, la facilidad de acceso y baja fricción: la disponibilidad de aplicaciones potentes en dispositivos

personales (BYOAI — *Bring Your Own AI*) permite una adopción instantánea sin intervención del departamento de TI [3,7]. Tercero, la laguna de gobernanza (*Governance Lag*): los ciclos de decisión y presupuesto en los grandes despachos (a menudo superiores a cuatro años) resultan excesivamente lentos frente a una innovación tecnológica que evoluciona mensualmente . Esta desconexión obliga a los profesionales a buscar sus propias soluciones de "auto-soporte" cognitivo . Cuarto, las señales ejecutivas contradictorias: en muchas firmas coexiste la presión de los socios por "experimentar con IA" para parecer innovadores ante el cliente con la ausencia de infraestructura segura para hacerlo, lo que los asociados interpretan como un permiso tácito para el uso de herramientas no autorizadas .

2.5. El concepto de "Erosión del Aseguramiento"

La consecuencia más grave del *Shadow AI* en la abogacía es la "erosión del aseguramiento" (*assurance erosion*) [3,7]. En un despacho de abogados, el aseguramiento es la capacidad de demostrar ante el cliente, los tribunales y las autoridades de protección de datos que se han mantenido los controles de confidencialidad y secreto [2].

El uso de transcriptores automáticos no autorizados rompe este esquema a través de tres vías diferenciadas [3]: el *bypass* de límites (*Boundary Bypass*), mediante el cual los datos de voz del cliente salen físicamente de los límites lógicos controlados por el despacho hacia nubes opacas [2]; la expansión de capacidad no evaluada, dado que las actualizaciones de software comunes incorporan "silenciosamente" funciones de IA que capturan audio o pantalla sin que el despacho haya realizado una EIPD [11]; y la pérdida de observabilidad, que priva a la firma de la capacidad forense para reconstruir un incidente, vulnerando el deber de responsabilidad proactiva del artículo 5.2 del RGPD [4].

En definitiva, el *Shadow AI* en el sector legal es el resultado de un desajuste entre la demanda operativa de eficiencia y la velocidad de respuesta de los marcos de *compliance*. No se trata de un problema tecnológico, sino de una crisis de soberanía operativa sobre la información del cliente [3,11].

3. Herramientas de transcripción y asistentes de notas no autorizados

3.1. Taxonomía de los asistentes de voz en el ecosistema legal

El mercado de la inteligencia artificial aplicada a la voz ha experimentado una explosión de soluciones que, si bien incrementan la productividad, operan mayoritariamente fuera del control de los departamentos de cumplimiento de los despachos. Es necesario clasificar estas herramientas en tres categorías principales según su modo de interacción y su nivel de integración en el flujo de trabajo [7,13]:

Primera categoría: bots de asistencia en videoconferencias. Son agentes de IA (como *Fireflies.ai*, *Otter.ai* o *Notta.ai*) que se unen a llamadas de plataformas como Microsoft Teams, Zoom o Google Meet como participante adicional [7,13]. Su función es capturar el flujo de audio en tiempo real, transcribirlo y generar resúmenes ejecutivos automáticos .

Segunda categoría: soluciones de infraestructura en la nube (*cloud-based*). Herramientas genéricas de grandes proveedores (como *Microsoft Azure Speech to Text*, *Google Cloud Speech-to-Text* o *Amazon Transcribe*) que los abogados emplean de forma *ad hoc* subiendo archivos de audio grabados previamente para obtener una versión escrita [13,19].

Tercera categoría: modelos de lenguaje de propósito general con capacidad de audio. La integración de modelos como *Whisper* de OpenAI o las capacidades de voz de *ChatGPT* y *Gemini* permite a los profesionales grabar notas de voz directamente en sus dispositivos personales y procesarlas mediante motores de IA generativa de consumo [13,20].

En el entorno de la abogacía española, el uso de estos asistentes es ya una realidad palpable. Según el *Libro Blanco sobre Inteligencia Artificial y Abogacía*, la transcripción automática y el reconocimiento de voz son utilizados por el 20,2% de los juristas que ya emplean IA, situándose como la segunda función más demandada tras los *chatbots* [13].

3.2. Análisis técnico de la arquitectura y flujos de datos opacos

La arquitectura técnica de las herramientas que componen el *Shadow AI* en transcripción presenta riesgos estructurales derivados de su naturaleza de "caja negra" [13]. La mayoría de estas aplicaciones operan bajo un modelo de *Software as a Service* (SaaS) en nubes públicas, lo que implica que el flujo de datos no solo sale del perímetro del despacho, sino que a menudo cruza fronteras jurisdiccionales [7,20].

El análisis de los tres componentes críticos de su arquitectura revela lo siguiente. En cuanto a la captura y transmisión: al unirse un bot a una reunión, actúa como un "oyente pasivo" que captura la señal de audio y la transmite —cifrada en el mejor de los casos— a los servidores del proveedor [19,20], sin que exista transparencia suficiente sobre quién tiene acceso a esos flujos de datos en tránsito . En cuanto al procesamiento mediante PLN: el audio se descompone en unidades fonéticas que son analizadas por modelos de Procesamiento de Lenguaje Natural para su conversión en texto estructurado [13]; este proceso consume una alta capacidad de computación que raramente se realiza de forma local en el dispositivo del abogado . En cuanto al almacenamiento y los metadatos: además de la transcripción, estas herramientas generan y almacenan metadatos críticos —direcciones IP de los participantes, duración de la llamada, identificadores de dispositivos y, en sistemas avanzados, análisis de sentimientos o expresiones faciales —, que la AEPD califica como datos personales merecedores del mismo nivel de protección que el contenido de la comunicación .

3.3. El problema del reentrenamiento y el procesamiento por terceros

El riesgo más insidioso del uso no autorizado de transcriptores es el destino final de la voz y el texto para el refinamiento de los algoritmos del proveedor. Como señala la AEPD en sus directrices de 2026, es práctica común en la industria que los datos recolectados se empleen para reentrenar modelos acústicos y lingüísticos [19,20]. Este riesgo de filtración presenta tres dimensiones:

La responsabilidad disociada: a menudo, el responsable de la transcripción no coincide con quien realiza el mantenimiento del sistema de IA. El proveedor del servicio puede actuar como responsable independiente para sus propios fines de mejora del modelo, escapando al control del abogado que introdujo los datos del cliente [20]. La supervisión humana por parte del proveedor: el entrenamiento de estos sistemas suele ser supervisado, lo que significa que fragmentos de las voces y transcripciones de reuniones confidenciales pueden ser escuchados o leídos manualmente por personal externo del proveedor tecnológico para corregir errores del algoritmo , circunstancia que rompe frontalmente el deber de secreto profesional [7]. La inferencia de información sensible: los servicios avanzados de transcripción pueden realizar tratamientos adicionales para inferir emociones, creencias o incluso el estado de salud de los clientes a partir de los patrones de voz, lo que entraría en la categoría de tratamientos de alto riesgo o incluso prohibidos por el Reglamento (UE) 2024/1689 .

3.4. La materialización del riesgo: Inexactitud y "alucinaciones" acústicas

Un aspecto técnico con profundas consecuencias jurídicas es la naturaleza probabilística de la transcripción por IA. Al no ser un proceso determinista, los sistemas son propensos a errores sistemáticos causados por ruidos de fondo, acentos regionales o el uso de jerga jurídica compleja [7,19]. La AEPD ejemplifica este riesgo de inexactitud —que vulnera el artículo 5.1.d) del RGPD— con un caso en el que una imprecisión acústica transcribió un nombre propio de forma ofensiva o errónea, alterando el sentido de una declaración judicial o estratégica . En un contexto legal, una transcripción incorrecta que atribuya a un cliente una admisión de responsabilidad que nunca pronunció puede derivar en responsabilidad civil por daños y perjuicios para el letrado . El uso de estas herramientas en la sombra elude la obligación de establecer procedimientos de revisión humana obligatoria antes de que el texto se incorpore al expediente del caso .

3.5. Transparencia técnica vs. Transparencia activa en reuniones

El consentimiento que un cliente otorga para una reunión se limita a la interacción profesional, pero el uso de un transcriptor no autorizado introduce un tratamiento de datos personales de voz cuya temporalidad y finalidad no suelen ser comunicadas [19]. El uso de estas herramientas vulnera el principio de transparencia reforzada por dos vías : primero, la ausencia de indicadores visuales continuos —el RGPD y las orientaciones de la AEPD de 2026 exigen indicadores visibles y activos durante toda la grabación —; segundo, la caducidad del consentimiento, puesto que las herramientas no supervisadas suelen carecer de mecanismos de desactivación automática fehaciente, pudiendo mantener canales de captura activos más allá del ámbito temporal autorizado por el cliente .

En conclusión, el uso de asistentes de notas no autorizados representa un "puente de plata" para la fuga de información confidencial hacia nubes opacas, donde la pérdida de soberanía operativa sobre el dato del cliente es absoluta y difícilmente reversible [7,11,20].

4. Impacto en el secreto profesional y el privilegio abogado-cliente

4.1. Naturaleza y dimensión constitucional del secreto en la era algorítmica

El secreto profesional y el privilegio abogado-cliente no constituyen meros estándares de cumplimiento técnico o requisitos de privacidad corporativa; representan garantías fundamentales de los derechos constitucionales a la defensa y a la tutela judicial efectiva, conformando la esencia ética de la abogacía [12,14]. En el ordenamiento jurídico español, esta protección ha alcanzado su máximo rango normativo mediante la Ley Orgánica 5/2024, de 11 de noviembre, del Derecho de Defensa, que en sus artículos 15 y 16 blinda la confidencialidad de las comunicaciones en el marco del encargo profesional, extendiendo expresamente la protección a "cualquier soporte digital" en que se contenga la información del cliente .

La irrupción del *Shadow AI* en las reuniones con clientes altera la naturaleza misma de esta protección. El secreto profesional se basa en una expectativa de exclusividad que se rompe cuando un tercero —el proveedor del sistema de IA no autorizado— accede al flujo de información [7,13]. El uso clandestino de transcriptores automáticos supone la introducción de un "tercero masivo" en la relación de confianza: un actor que no solo almacena la información, sino que la procesa y, en los modelos de consumo, la integra en su base de conocimiento global [10,12]. La reserva de humanidad que exige la ley queda desplazada por una delegación tecnológica invisible que el cliente raramente comprende en su totalidad .

4.2. La doctrina del "abandono negligente" y la irreversibilidad de la pérdida del privilegio

Para dimensionar la gravedad del riesgo, procede recurrir a la doctrina ética comparada. La American Bar Association (ABA) ha sido pionera en advertir que procesar datos de un caso en un motor de IA comercial sin controles de privacidad estrictos es un acto negligente [14], asimilable a "abandonar expedientes físicos desatendidos en un vagón de tren" [7]. En ambos casos, el profesional renuncia de facto al control sobre la información, permitiendo que cualquier tercero acceda a ella .

Un aspecto especialmente crítico es la irreversibilidad de la pérdida de confidencialidad. Una vez que el privilegio abogado-cliente se rompe por una divulgación negligente a un tercero no protegido por el secreto, la información pierde su estatus de protección especial [14]. En un litigio ordinario, la contraparte podría solicitar la exhibición de las transcripciones almacenadas en la nube del proveedor de IA, alegando que el abogado, al usar una herramienta pública, ha

renunciado implícitamente a la protección del secreto [7]. Este escenario representa una amenaza existencial para la estrategia de defensa de cualquier despacho.

4.3. Riesgos "intraoficina" y el quiebre de las murallas éticas (_Ethical Walls_)

El fenómeno del *Shadow AI* no solo proyecta riesgos hacia el exterior de la firma, sino que genera vulnerabilidades internas de alta complejidad. Los denominados "riesgos intraoficina" derivan de la falta de aislamiento en la infraestructura de IA [15]: si un despacho no utiliza entornos empresariales segregados, los datos introducidos como instrucciones (*prompts*) o los audios de reuniones por parte de un equipo de abogados pueden incorporarse a la memoria contextual del modelo o a sus pesos ajustados [16].

Esta circunstancia puede provocar que información confidencial de un caso específico emerja como respuesta (*output*) ante una consulta ordinaria de otro profesional de la misma firma que trabaje para un cliente con intereses contrapuestos [15], vulnerando directamente las murallas éticas de protección establecidas por las normas de conducta profesional para gestionar conflictos de interés . La opacidad de los algoritmos de IA en la sombra hace técnicamente imposible que el departamento de *compliance* rastree si se ha producido esta polinización cruzada de secretos de clientes [7].

4.4. Evolución de la regulación deontológica en España: Las tres Circulares (2025-2026)

La relevancia de proteger el secreto profesional en entornos digitales ha motivado una respuesta normativa sin precedentes por parte del Consejo General de la Abogacía Española (CGAE), articulada a través de tres Circulares deontológicas progresivas [16].

La Circular 1/2025 (noviembre) se dedicó íntegramente a la protección del secreto profesional en entornos de computación en la nube, advirtiendo que la exposición de datos ante tecnologías no auditadas conlleva responsabilidades civiles y disciplinarias directas [16]. La Circular 2/2026 (enero), aunque centrada en la gestión de fondos, reforzó el deber de custodia integral de toda la información patrimonial y sensible del cliente frente a asistentes inteligentes de gestión . La Circular 3/2026 (aprobada el 10 de abril de 2026) regula específicamente el uso de IA generativa en la redacción y gestión de textos profesionales, subrayando que la IA es una herramienta auxiliar que nunca debe operar como sustituto del abogado y exigiendo una supervisión humana extrema para evitar "alucinaciones" que comprometan el celo profesional [5].

Este marco normativo establece una obligación de resultado para el letrado: el abogado es siempre el responsable último de garantizar que ningún dato

identificable del cliente sea procesado por sistemas que no ofrezcan garantías contractuales de no-reutilización [5,13,16].

4.5. Estándares internacionales y el deber de competencia tecnológica

A nivel internacional, la tendencia es inequívoca: la "competencia tecnológica" se consolida como un deber deontológico autónomo. El Consejo de Colegios de la Abogacía de Europa (CCBE) y la *Solicitors Regulation Authority* (SRA) del Reino Unido exigen que los abogados comprendan los fundamentos técnicos de las herramientas que utilizan [17]. Esta obligación implica que el desconocimiento del modo en que un asistente de notas gestiona la privacidad no sirve como eximente ante un error del sistema o una filtración . El CCBE recuerda que los abogados asumen plena responsabilidad por las deficiencias del servicio, incluso si estas derivan de un fallo en un sistema opaco de IA .

En el plano convencional, resulta ineludible mencionar el Convenio Marco sobre Inteligencia Artificial y Derechos Humanos, Democracia y Estado de Derecho (CETS núm. 225), abierto a la firma en Vilnius el 5 de septiembre de 2024 y que constituye el primer tratado internacional jurídicamente vinculante sobre inteligencia artificial [24]. El Convenio impone a las Partes la obligación de velar por que los sistemas de IA que afecten a derechos fundamentales sean diseñados y utilizados con garantías de transparencia, supervisión humana y rendición de cuentas . Aunque su ámbito de aplicación directo alcanza principalmente al sector público, su impacto como estándar de referencia para el ejercicio privado de la abogacía —en cuanto actividad que incide sobre los derechos constitucionales de los ciudadanos— es innegable [17].

El uso de *Shadow AI* constituye una infracción cualificada del deber de competencia tecnológica, pues el profesional no solo utiliza una herramienta compleja, sino que lo hace eludiendo activamente los controles de seguridad diseñados para proteger el secreto [7,17].

4.6. Conclusión de la sección: El secreto como límite absoluto

El secreto profesional actúa como límite absoluto e infranqueable para el uso de la IA en la sombra. La eficiencia es un objetivo deseable, pero nunca puede alcanzarse a costa de la pérdida de soberanía operativa sobre el dato del cliente [13,18]. La única vía compatible con la ética profesional es la migración obligatoria hacia entornos de "IA por diseño", donde la confidencialidad no sea una opción configurable, sino una restricción técnica impuesta por la arquitectura del sistema [3,11].

5. Infracciones al RGPD y a la LOPDGDD

5.1. La condición de responsable del tratamiento y la ruptura de la cadena de mando

El despliegue de herramientas de transcripción en la sombra dentro de un despacho de abogados no solo representa una quiebra de la política interna, sino que altera la arquitectura de responsabilidad jurídica definida por el RGPD. De acuerdo con las directrices de la AEPD de abril de 2026, cualquier firma legal que incorpore un sistema de transcripción automática —ya sea por decisión institucional o por tolerancia ante la iniciativa individual de sus asociados— asume plenamente la condición jurídica de responsable del tratamiento [7,19].

Esta atribución implica que la firma es la entidad que determina los fines y los medios del tratamiento [19]. El fenómeno del *Shadow AI* genera una "ruptura de la cadena de mando" normativa: el abogado utiliza el asistente de IA para un fin profesional (transcribir una reunión), pero al eludir los canales de supervisión, impide que el despacho cumpla con su deber de diligencia debida en la selección de encargados del tratamiento conforme al artículo 28 del RGPD [7,20]. La AEPD advierte que esta diligencia no es un trámite estático, sino un deber de supervisión continuo durante todo el ciclo de vida de la herramienta . El uso no autorizado imposibilita la evaluación previa de metadatos, *logs* de conexión y, de forma crítica, la verificación de si el proveedor utiliza las muestras de voz para reentrenar sus propios modelos .

5.2. Bases jurídicas de legitimación: El fracaso del consentimiento y del interés legítimo

El uso de transcriptores en la sombra suele carecer de una base jurídica válida bajo el artículo 6 del RGPD, incurriendo en tratamientos ilícitos de datos personales [7,19].

El consentimiento viciado. La práctica común de informar que "al unirse a la reunión se acepta la grabación" ha sido rechazada por la AEPD en resoluciones recientes (como la PS/00342/2023), al no cumplir con la exigencia de una manifestación de voluntad libre, específica, informada e inequívoca [19]. En el entorno del *Shadow AI*, el cliente ignora con frecuencia que su voz está siendo procesada por un motor de IA de terceros, lo que invalida cualquier consentimiento presunto [7]. La caducidad del consentimiento. El consentimiento para grabar una conversación es de carácter estrictamente finalista y temporal : las herramientas no supervisadas suelen carecer de mecanismos de desactivación automática fehaciente, lo que constituye una infracción grave . El test de ponderación del interés legítimo. Aunque algunos despachos intentan ampararse en el interés legítimo para mejorar la eficiencia operativa, la literatura técnica advierte que este interés raramente prevalece frente a los derechos y

libertades del interesado cuando se utilizan sistemas de IA opacos que capturan datos biométricos de voz [11,20].

5.3. El principio de exactitud y sus consecuencias procesales y civiles

Un aspecto crítico que la normativa de protección de datos proyecta sobre el sector legal es el principio de exactitud (artículo 5.1.d) del RGPD) [7,19]. La transcripción automática no es un texto neutral, sino una representación atribuida a una persona física identificable [20]. Los sistemas de IA generativa y de procesamiento de lenguaje natural son inherentemente probabilísticos y propensos a errores sistemáticos .

La AEPD ilustra el impacto de estos fallos técnicos en el ámbito jurídico con un caso real (anonimizado) en el que una imprecisión acústica transcribió erróneamente un apellido de forma ofensiva [19]. En un contexto de asesoramiento estratégico o litigioso, una inexactitud fonética de este calibre —o una "alucinación" que atribuya al cliente una admisión de responsabilidad inexistente— no solo vulnera el RGPD, sino que deriva en responsabilidad civil por daños y perjuicios para el letrado y el despacho [7]. La normativa exige que el responsable establezca medidas técnicas específicas, como la revisión humana obligatoria antes de que cualquier transcripción se incorpore a un expediente oficial o escrito procesal [16].

5.4. Vulneración del principio de transparencia y derechos de los interesados

El uso de asistentes de notas no autorizados supone un fallo sistémico en la transparencia activa [7]. La transparencia en la captura de voz no puede limitarse a una información previa puntual; requiere una transparencia reforzada [19]. El RGPD y las orientaciones de la AEPD de 2026 exigen que, durante toda la grabación, exista un indicador visible y activo que garantice que los participantes mantengan la conciencia plena de estar siendo grabados . Las herramientas en la sombra suelen ocultar su presencia tras avisos iniciales fugaces. Asimismo, bajo el artículo 15 del RGPD, el cliente tiene derecho a acceder a la transcripción de su conversación : cuando los despachos alegan "dificultades técnicas" para negar este acceso, incurren en una infracción, pues el responsable debe utilizar tecnologías de anonimización o difuminado de voz para salvaguardar los derechos de terceros sin menoscabar el derecho de acceso del interesado .

5.5. Transferencias internacionales de datos: El riesgo de la nube opaca

La mayoría de las herramientas que conforman el ecosistema del *Shadow AI* (como *Otter.ai* o *Fireflies.ai*) operan bajo infraestructuras de computación en la

nube situadas en jurisdicciones extranjeras, principalmente en Estados Unidos [7,18]. El uso de estas herramientas por parte de un abogado español conlleva un riesgo masivo de transferencias internacionales de datos ilícitas [13].

Si el despacho no ha contratado una modalidad *Enterprise* que garantice la residencia de los datos en el Espacio Económico Europeo (EEE), los flujos de audio y metadatos pueden quedar expuestos a accesos gubernamentales amparados en normativas como la *CLOUD Act* estadounidense [18]. El uso de licencias individuales de consumo público no ofrece las garantías contractuales de "no-reutilización" exigidas para cumplir con el estándar establecido por la STJUE de 16 de julio de 2020, *Data Protection Commissioner c. Facebook Ireland Ltd y Maximillian Schrems*, C-311/18 (Schrems II), y el posterior Marco de Privacidad UE-EE.UU. (*Data Privacy Framework*). Aunque este último no ha sido anulado, su vigencia no exime de realizar una evaluación caso por caso de las transferencias, conforme al artículo 46 del RGPD y la jurisprudencia del Tribunal de Justicia de la Unión Europea [7,15].

5.6. Tratamientos de alto riesgo e inferencia de información sensible

Algunos servicios de IA analizan patrones de voz para inferir emociones, estados de salud o rasgos de personalidad de los participantes [13,20]. Estos tratamientos pueden constituir el procesamiento de categorías especiales de datos (biométricos, de salud) sin una base legal reforzada ; entran en la categoría de tratamientos de alto riesgo que obligan al despacho a realizar una EIPD antes de su uso [16]; y podrían incurrir en prácticas prohibidas o restringidas bajo el Reglamento (UE) 2024/1689 si se utilizan para el reconocimiento de emociones en entornos laborales o profesionales sin una justificación de seguridad estricta .

En conclusión, el uso de herramientas de transcripción no autorizadas convierte al despacho en un infractor reactivo de la normativa de protección de datos, exponiéndolo a sanciones administrativas que, bajo el RGPD, pueden alcanzar cuantías de hasta 20 millones de euros o el 4% del volumen de negocio anual global, además del incalculable daño reputacional derivado de una brecha de confidencialidad de sus clientes [7,18].

6. El AI Act aplicado a despachos de abogados

6.1. Marco normativo: El Reglamento (UE) 2024/1689 como estándar global

La gobernanza de la inteligencia artificial en la abogacía europea ha entrado en una nueva fase de obligatoriedad tras la plena vigencia del Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, de 13 de junio de 2024 (en adelante, RIA o Reglamento de IA) [22]. Procede interpretar este Reglamento no como una norma técnica aislada, sino como un pilar infraestructural que, junto con el RGPD y la Ley Orgánica del Derecho de Defensa, redefine el estándar de diligencia profesional exigible a las firmas jurídicas [12,13].

El RIA adopta un enfoque basado en el riesgo, clasificando los sistemas de IA en cuatro niveles (inaceptable, alto, limitado y mínimo), e impone obligaciones diferenciadas según la posición del actor en la cadena de valor [22]. En el contexto de un despacho de abogados, la firma actúa mayoritariamente como desplegador (*deployer*), definido en el artículo 3, apartado 4, del RIA como la persona física o jurídica que utiliza un sistema de IA bajo su propia autoridad . Esta condición jurídica conlleva responsabilidades proactivas sustanciales, especialmente cuando el uso de la IA —en la sombra o autorizada— afecta a derechos fundamentales de los clientes o a la integridad de la administración de justicia [21].

6.2. Clasificación de riesgos en el ejercicio de la abogacía

Para valorar el impacto del RIA en los despachos, es preciso realizar un test de clasificación de los sistemas habitualmente empleados, advirtiendo que el *Shadow AI* elude precisamente esta categorización obligatoria [3,22].

Riesgo inaceptable (prácticas prohibidas). Bajo el artículo 5 del RIA, quedan prohibidos los sistemas que realicen una puntuación social o una categorización biométrica que infiera creencias políticas o identidades sensibles [22]. Los transcriptores avanzados que intenten predecir la veracidad del testimonio de un cliente mediante análisis biométrico de voz podrían incurrir en estas prohibiciones si se utilizan de forma no autorizada en entornos de interrogatorio o evaluación de riesgos [13].

Alto riesgo (Anexo III). Esta es la categoría más crítica para el sector legal. El Anexo III del RIA clasifica como de alto riesgo los sistemas de IA destinados a ser utilizados por una autoridad judicial para asistir en la investigación de hechos o la interpretación de la ley [21,22]. Aunque los despachos privados no son "autoridades judiciales", el uso de herramientas predictivas de sentencias para condicionar la estrategia de defensa podría entrar en una zona de alta sensibilidad regulatoria [5,13].

Riesgo limitado (obligaciones de transparencia). Aquí se sitúan la mayoría de los asistentes de notas, bots de transcripción y *chatbots* de atención al cliente [22]. El artículo 50 del RIA impone la obligación de informar a las personas físicas de que están interactuando con un sistema de IA, salvo que sea obvio por el contexto . El uso de un bot de transcripción en la sombra que no se identifique claramente ante el cliente vulnera directamente esta obligación [7]. Riesgo mínimo: herramientas de ofimática con IA básica que no interactúan directamente con la toma de decisiones .

6.3. La alfabetización en IA como deber legal (artículo 4 RIA)

Una de las novedades más relevantes para los recursos humanos de las firmas legales es el deber de alfabetización en IA consagrado en el artículo 4 del RIA [22]. El Reglamento exige que los desplegadores adopten medidas para garantizar que su personal tenga un nivel de conocimientos suficiente para comprender el funcionamiento, los riesgos y las limitaciones de los sistemas de IA que utilizan .

Esta obligación legal refuerza el deber de competencia tecnológica ya señalado por la Circular 3/2026 del CGAE [5,16]. Un despacho que tolere el *Shadow AI* entre sus asociados está incumpliendo el artículo 4 del RIA, pues no puede certificar la alfabetización de sus empleados sobre herramientas cuya existencia ignora [3,7,22]. La formación continua no es ya solo una recomendación de buenas prácticas [6,13], sino un requisito de cumplimiento normativo que el despacho debe documentar bajo el principio de responsabilidad proactiva (*accountability*) [11].

6.4. Supervisión humana y soberanía operativa (artículo 14 RIA)

El artículo 14 del RIA establece que los sistemas de IA de alto riesgo deben estar diseñados para permitir una supervisión humana efectiva que prevenga o reduzca al mínimo los riesgos para los derechos fundamentales [22]. En el entorno de la transcripción automática de reuniones, este mandato se traduce en la prohibición de la "delegación decisoria" [13,21]. La Instrucción 2/2026 del CGPJ, tomada como estándar orientativo de máxima referencia para la abogacía , subraya que la IA debe operar únicamente como instrumento de apoyo, manteniendo el profesional la responsabilidad plena y exclusiva de la validación crítica de los resultados . El uso de transcriptores en la sombra anula esta supervisión: si el despacho desconoce que se está utilizando un bot, no puede articular el procedimiento de revisión humana obligatoria exigido por el Reglamento, permitiendo que "alucinaciones" o errores acústicos se incorporen de forma invisible al expediente judicial [7,19].

Procede señalar, en este contexto, la relevancia del artículo 86 del RIA, que establece un derecho autónomo a la explicación de las decisiones individuales adoptadas por sistemas de IA de alto riesgo. Este derecho opera con independencia del artículo 22 del RGPD y amplía el estándar de transparencia

exigible al desplegador: la firma jurídica que utilice sistemas de IA para apoyar decisiones que afecten a los derechos o intereses del cliente debe estar en condiciones de explicar, de forma significativa, la lógica de esas decisiones. Ello resulta técnicamente imposible cuando se emplean herramientas en la sombra cuya arquitectura y proceso decisorio el despacho desconoce.

6.5. Gobernanza de datos y transparencia en modelos de propósito general

Para los despachos que utilicen sistemas basados en modelos de lenguaje de gran tamaño (como ChatGPT, Claude o asistentes de voz basados en modelos fundacionales), el RIA impone obligaciones adicionales de transparencia a los proveedores (artículos 52 y 53), que el despacho debe verificar en su diligencia debida [22]. El cumplimiento del RIA exige: un inventario de activos de IA que haga imposible cumplir con el Reglamento sin un registro exhaustivo de las herramientas en uso [11]; una evaluación de impacto en derechos fundamentales, cuya realización el *Libro Blanco sobre IA y Abogacía* recomienda ante tratamientos que afecten al secreto profesional [13]; y transparencia reforzada mediante indicadores activos durante la interacción [19].

6.6. Régimen sancionador: La "multa por Shadow AI"

El artículo 99 del RIA —y no el artículo 71, que correspondía a la numeración de la propuesta de la Comisión de 2021, superada por la versión definitiva publicada en el DO L 2024/1689— establece cuantías sancionadoras disuasorias que pueden alcanzar los 35 millones de euros o el 7% del volumen de negocio anual global por el uso de prácticas prohibidas [22]. Para los despachos, el mayor riesgo reside en las multas por infracción de las obligaciones de transparencia y gobernanza de datos .

El uso de IA en la sombra no será tratado por las autoridades de control como un error individual del abogado, sino como un fallo sistémico en la supervisión de la firma [7,11]. Bajo el RIA, la falta de control sobre las herramientas que utilizan sus empleados constituye una infracción de los deberes de supervisión del desplegador, agravada por la posible opacidad en las transferencias internacionales de datos que estas herramientas realizan hacia nubes no auditadas [18,22].

En conclusión, el RIA transforma la gobernanza de la IA en los despachos de una opción ética en un imperativo legal de cumplimiento. La soberanía operativa sobre el dato del cliente —perdida en el fenómeno del *Shadow AI*— debe ser recuperada mediante marcos de observabilidad técnica que permitan al despacho certificar ante el regulador que cada palabra transcrita está bajo control humano y protegida por un entorno de diseño seguro [3,11,22].

7. Casos reales y sanciones relevantes (2024-2026)

7.1. De la fase de experimentación a la fase de responsabilidad: El fin de la impunidad

La transición del sector legal hacia la inteligencia artificial ha estado marcada por un cambio drástico en el clima regulatorio. Si el año 2023 se caracterizó por la curiosidad y la experimentación desordenada, el periodo comprendido entre 2024 y el primer semestre de 2026 ha sido el de la materialización de la responsabilidad profesional [13,22]. La jurisprudencia y las resoluciones administrativas recientes han enviado un mensaje inequívoco: el desconocimiento técnico no es una eximente de la negligencia profesional [4].

7.2. Sanciones por "alucinaciones" y falta de supervisión humana

El riesgo de las "alucinaciones" —generación de información plausible pero falsa por parte de los modelos de lenguaje— ha pasado de ser una advertencia técnica a una causa recurrente de sanciones disciplinarias y procesales [7,13].

El caso *Avianca v. Roberto Mata* (2023-2024, EE.UU.) consolidó en 2024 una doctrina de alcance global [13]. El tribunal del Distrito Sur de Nueva York impuso una sanción económica de 5.000 dólares a un equipo de abogados que utilizó ChatGPT para localizar jurisprudencia, resultando en la citación de más de una decena de decisiones judiciales inexistentes . El tribunal subrayó que, si bien el uso de IA no está prohibido, la obligación del letrado de verificar la veracidad de cada fuente es absoluta e indelegable .

El Auto del Tribunal Superior de Justicia de Navarra (ATSJ NA 38/2024) marcó un precedente crítico en España [13]. Un abogado incorporó en una querella referencias al Código Penal de la República de Colombia debido a un "manejo inadecuado" de ChatGPT . La Sala archivó la pieza separada sin sanción económica tras la disculpa y rectificación del letrado, pero el Auto operó como una "advertencia institucional" sobre las implicaciones deontológicas del uso descuidado de la IA .

La Nota Informativa 90/2024 del Tribunal Constitucional (septiembre de 2024) impuso una sanción de apercibimiento a un abogado que presentó una demanda de amparo con 19 citas entrecomilladas de sentencias del propio tribunal que resultaron ser irreales [13]. El tribunal rechazó la alegación de "desconfiguración de base de datos", recordando que el abogado es siempre el responsable último de la revisión exhaustiva del contenido antes de su presentación .

7.3. Protección de consumidores y ejercicio ilícito: El caso DoNotPay

El fenómeno de los "abogados robot" ha sido objeto de una ofensiva regulatoria por parte de las autoridades de competencia y consumo [13]. En febrero de 2025, la Comisión Federal de Comercio de los Estados Unidos (FTC) emitió una orden definitiva que obligaba a la plataforma DoNotPay al pago de 193.000 dólares por publicidad engañosa . La FTC determinó que la empresa se promocionaba como sustituto legal sin respaldo técnico real, careciendo de abogados cualificados que supervisaran los servicios prestados . Desde una perspectiva de cumplimiento, el caso es relevante también por abordar la confidencialidad: la política de privacidad de la plataforma excluía expresamente la protección del secreto profesional, exponiendo los datos de los usuarios ante terceros sin consentimiento informado .

7.4. Resoluciones de la AEPD: El consentimiento y la transparencia en la captura de voz

La AEPD ha intensificado la vigilancia sobre la captura no autorizada de flujos de audio en entornos profesionales [11,19]. La Resolución PS/00342/2023 (consolidada en 2024) sentó el criterio de que el mero hecho de unirse a una reunión tras un aviso genérico de grabación no constituye un consentimiento válido bajo el RGPD : la manifestación de voluntad del cliente debe ser libre, específica e inequívoca [7]. Siguiendo las orientaciones publicadas en abril de 2026, la AEPD ha iniciado procedimientos de apercibimiento contra firmas profesionales que emplean sistemas de transcripción sin transparencia reforzada, exigiendo indicadores visuales o sonoros activos y continuos durante toda la sesión .

7.5. El impacto forense del Shadow AI: Pérdida de observabilidad y multas por brechas de datos

Un riesgo materializado en el último bienio es la incapacidad de los despachos para reconstruir incidentes de seguridad debido al uso de IA en la sombra. La literatura técnica describe casos en los que, ante una sospecha de filtración de información confidencial, el departamento de *compliance* fue incapaz de auditar lo ocurrido porque el asociado responsable había procesado los audios en un asistente de notas personal [3,9]. Este escenario constituye una infracción del principio de responsabilidad proactiva del artículo 5.2 del RGPD [4,19]. La AEPD ha señalado que la pérdida de soberanía operativa sobre el dato del cliente agrava cualquier sanción por brecha de datos [11,18]: si un despacho no puede demostrar qué IA se utilizó ni qué medidas de seguridad aplicaba el tercero, el regulador asume que no existió diligencia debida en la custodia de la información .

7.6. Instrucción 2/2026 del CGPJ: El estándar de la judicatura como referencia para la abogacía

La Instrucción 2/2026 del Consejo General del Poder Judicial sobre el uso de IA en la actividad jurisdiccional establece el listón de calidad que los abogados deben esperar y replicar [21]. La Instrucción prohíbe taxativamente incorporar datos judiciales no públicos a herramientas de IA externas y exige un "control humano efectivo" que impida la delegación decisoria . Su proyección sobre la abogacía opera como estándar orientativo de máxima referencia y no como norma jurídicamente obligatoria para los letrados . El incumplimiento de estos principios por parte de un abogado —por ejemplo, al presentar un escrito generado íntegramente por IA sin supervisión— está siendo tratado por los tribunales como una vulneración de la buena fe procesal [13]. La jurisprudencia del Tribunal Superior de Londres (2024) ha consolidado el deber de los abogados de llamar la atención del tribunal sobre el uso de IA en sus escritos, asimilando la ocultación de este hecho a un intento de inducir a error al órgano judicial .

7.7. Conclusión de la sección: Hacia un cumplimiento preventivo

El catálogo de casos entre 2024 y 2026 demuestra que el *Shadow AI* ha dejado de ser un riesgo hipotético para convertirse en una fuente de sanciones pecuniarias, disciplinarias y procesales reales [11,13]. La lección extraída de estos precedentes es que la adopción de la IA en la abogacía debe ser institucional, transparente y supervisada [5,22]. El uso *ad hoc* de herramientas en la sombra no solo vulnera el secreto profesional, sino que sitúa al letrado en una posición de vulnerabilidad absoluta ante el regulador y los tribunales [3].

8. Responsabilidad profesional y cobertura aseguradora

8.1. El fin de la "infalibilidad técnica" y la exigencia de responsabilidad proactiva

La adopción estructural de la inteligencia artificial en los despachos ha provocado una mutación en el régimen de responsabilidad profesional de los abogados. Se ha transitado de un escenario de "curiosidad tecnológica" a uno de "responsabilidad operativa total", donde el abogado ya no puede ampararse en la opacidad del sistema para justificar un error [12,13]. Bajo el marco del RIA y el principio de responsabilidad proactiva del RGPD, el despacho asume una obligación de supervisión técnica que es indelegable [11,22].

El uso de herramientas de *Shadow AI* sitúa a la firma en una posición de vulnerabilidad jurídica extrema. Ante un sistema corporativo auditado, el despacho puede demostrar que ejerció la diligencia debida en la selección del proveedor conforme al artículo 28 del RGPD; el uso clandestino de herramientas por parte de asociados o empleados anula esta defensa [7,19]. La responsabilidad profesional en 2026 se mide por la capacidad de la firma para mantener la "soberanía operativa" sobre el flujo de datos del cliente, soberanía que se pierde irremediablemente cuando la información se introduce en motores de IA de consumo cuyos términos de servicio el despacho desconoce [10,12].

8.2. El deber de supervisión y la "reserva de humanidad"

El principio de supervisión humana efectiva consagrado en el artículo 14 del RIA se ha convertido en el nuevo estándar de oro de la diligencia debida en la abogacía [22]. Este deber se traduce en la "reserva de humanidad": la prohibición absoluta de que un sistema de IA asuma por sí solo decisiones jurídicas o procesales sin una validación crítica y humana [13,21]. La Circular 3/2026 del CGAE eleva este principio a la categoría de obligación deontológica reforzada [12], complementada por la Circular 1/2025, que ya advirtió sobre la necesidad de proteger el secreto profesional en entornos de computación en la nube [16].

El deber de supervisión presenta tres dimensiones que afectan directamente a la responsabilidad del letrado. Primera: el deber de validación crítica obliga al abogado a revisar íntegramente cada transcripción o borrador generado por IA [12]; como señala el Tribunal Constitucional en su Nota 90/2024, alegar un "error del algoritmo" no exime de responsabilidad [13]. Segunda: la responsabilidad por "alucinaciones" implica que los errores sistemáticos de los modelos probabilísticos se consideran, a efectos de responsabilidad civil, como una falta de cuidado razonable en la prestación del servicio [17]; la negligencia no reside en que la IA cometa el error, sino en que el abogado no lo detecte . Tercera: la

vigilancia del *Shadow AI* hace que los socios y directores de las firmas asuman una responsabilidad vicaria por el uso de IA no autorizada en sus equipos .

8.3. Responsabilidad civil profesional ante el error algorítmico

El régimen de responsabilidad civil en la abogacía se enfrenta al desafío de cuantificar los daños derivados de fallos técnicos complejos. La responsabilidad por el uso de IA en la sombra no se limita al ámbito disciplinario, sino que proyecta consecuencias patrimoniales directas ante el cliente [13,17]. Cabe identificar dos escenarios principales de materialización del riesgo [7,19]: el perjuicio procesal por inexactitud —si un asistente de notas transcribe erróneamente una admisión de responsabilidad o una cifra clave en una negociación, y el abogado incorpora ese error a un documento con efectos jurídicos, la firma responde por el daño causado al derecho de defensa del cliente —; y la pérdida del privilegio abogado-cliente —el uso negligente de IA de consumo que provoque una filtración de secretos industriales o de la estrategia procesal puede ser calificado como "abandono de expedientes" [14], dando lugar a reclamaciones por pérdida de oportunidad o daño reputacional .

8.4. La respuesta del mercado asegurador: Cláusulas de exclusión y ciberseguros

La proliferación del *Shadow AI* ha provocado una reacción defensiva por parte de las compañías aseguradoras. Se detecta una tendencia hacia la exclusión sistemática de cobertura para incidentes derivados del uso de herramientas de IA que no figuren en el inventario formal de activos digitales del despacho [11,13]: las aseguradoras argumentan que no pueden cubrir riesgos derivados de nubes públicas cuyos estándares de seguridad no han sido evaluados por la firma [8]. Algunas pólizas comienzan a supeditar la cobertura a que el despacho demuestre que su personal ha recibido la formación obligatoria exigida por el artículo 4 del RIA [22]; la falta de capacitación técnica del asociado que usó un transcriptor en la sombra puede ser utilizada por la aseguradora para alegar "culpa grave" . El riesgo del *Shadow AI* se sitúa en la intersección entre la responsabilidad civil profesional y el ciberriesgo : las aseguradoras exigen ahora la articulación de medidas técnicas proactivas —como el Esquema Nacional de Seguridad (ENS)— para mantener activas las coberturas ante fugas de información [15].

8.5. Hacia un estándar de "Seguro por Diseño" (_Insurance by design_)

Los despachos deben evolucionar hacia un modelo de "seguro por diseño", donde la contratación de herramientas de IA se valide no solo por TI y Cumplimiento, sino también por el bróker de seguros de la firma [11]. La adopción de IA autorizada en modalidades *Enterprise* no es solo una medida de eficiencia,

sino una garantía de mantenimiento de la cobertura aseguradora, al ofrecer las cláusulas de "no-reutilización de datos" que las pólizas exigen para cubrir incidentes de confidencialidad [2,5,13]. La literatura técnica del primer semestre de 2026 subraya que el departamento de *compliance* debe certificar periódicamente ante la aseguradora la ausencia de *Shadow AI* en los procesos críticos [3], para lo cual resulta imprescindible contar con marcos de observabilidad que generen bitácoras de auditoría (*AI Verification Logs*) capaces de reconstruir cualquier incidente [7].

8.6. Conclusión de la sección: La responsabilidad como barrera contra la sombra

La responsabilidad profesional es hoy la barrera más sólida frente al fenómeno del *Shadow AI*. La firma no puede permitir que sus abogados busquen "auto-soporte" en herramientas externas opacas, pues ello anula su capacidad de defensa ante el regulador y de cobertura ante su aseguradora [3,7,13]. La soberanía operativa sobre el dato del cliente es el único camino compatible con la viabilidad económica y ética del despacho en la era del RIA [11,22].

9. Estrategias de compliance y gobernanza preventiva

9.1. El cambio de paradigma: Del cumplimiento declarativo a la observabilidad técnica

La mitigación eficaz del fenómeno del *Shadow AI* exige que los despachos de abogados abandonen la postura tradicional de emitir prohibiciones genéricas en sus manuales corporativos y adopten, en su lugar, un modelo dinámico de cumplimiento normativo y observabilidad proactiva [3,7,23]. El modelo clásico de *compliance*, basado en atestaciones humanas y cuestionarios periódicos, ha quedado obsoleto ante la velocidad y opacidad de las integraciones de IA . Mientras que el departamento de cumplimiento puede tener protocolos declarativos alineados con la normativa, la falta de herramientas de telemetría capaces de detectar llamadas a interfaces de programación de aplicaciones (API) no autorizadas genera una brecha de observabilidad profunda .

La soberanía operativa real sobre el dato del cliente solo se recupera mediante un marco de "gobernanza por diseño" [3,11]: el despliegue de agentes de extracción de observabilidad que inspeccionen continuamente los flujos de datos y metadatos de las herramientas utilizadas por los asociados es la única vía para identificar sistemas no declarados en el inventario de activos digitales antes de que se produzca una filtración irreversible [16].

9.2. Fase 1: Descubrimiento y auditoría de red (Zero-Trust Telemetry)

La primera fase de una estrategia de gobernanza preventiva debe centrarse en el descubrimiento activo [7]. Es esencial que los departamentos de TI articulen herramientas de telemetría basadas en auditorías de tráfico API para identificar en tiempo real qué asistentes de voz y transcriptores están operando de manera clandestina [3]. Bajo un modelo de arquitectura de seguridad *Zero-Trust* , el despacho debe partir de la premisa de que ningún sistema o proceso merece confianza por defecto, con independencia de si opera dentro o fuera del perímetro de la firma . Esta fase requiere: el mantenimiento de un inventario automatizado de todos los sistemas de IA en uso, documentando su finalidad, propietario responsable y nivel de riesgo bajo el RIA [22]; la articulación de sondas de validación efímeras que verifiquen la configuración de seguridad de las herramientas sin ingresar al contenido de los mensajes o audios ; y la detección de "*Usecase Drift*" para monitorizar si una herramienta autorizada para tareas de bajo riesgo está siendo utilizada de forma anómala para procesar datos sensibles de clientes .

9.3. Fase 2: Homologación de entornos protegidos y políticas BYOAI

Una vez mapeada la superficie de uso, el despacho debe sustituir la opacidad por la homologación [7]. La prohibición absoluta de la IA es contraproducente, pues tiende a desplazar el uso hacia dispositivos personales fuera del control institucional [3,23]. La estrategia recomendada es la provisión de entornos de trabajo protegidos (*sanitized environments*) [13]. La firma debe contratar licencias en modalidad *Enterprise* que incluyan cláusulas de gobernanza robustas [10], en particular: la prohibición de reentrenamiento (el proveedor debe garantizar por contrato que los audios, transcripciones y *prompts* no se utilizarán para mejorar sus modelos comerciales) ; la residencia de datos en el EEE para evitar infracciones por transferencias internacionales ilícitas [11,18]; y la capacidad de auditoría mediante la generación de bitácoras de actividad (*logs*) que permitan reconstruir cualquier incidente . Asimismo, la política BYOAI debe delimitar con claridad qué perfiles profesionales pueden interactuar con cada herramienta, reservando el procesamiento de datos sensibles a abogados formados en sistemas corporativos seguros .

9.4. Fase 3: Compliance en reuniones y transparencia reforzada

Para el uso específico de asistentes de notas en reuniones con clientes, el despacho debe articular protocolos de transparencia reforzada, alineados con las directrices de la AEPD de abril de 2026 [19]. Un aviso de grabación genérico al inicio de la sesión resulta insuficiente . La hoja de ruta operativa propuesta incluye: facilitar al cliente una plantilla informativa que detalle qué motor de IA concreto procesará la grabación, sus riesgos y el tiempo de conservación [11]; configurar la plataforma de videoconferencia para que muestre un aviso persistente en pantalla o una señal luminosa durante todo el tiempo que el canal de captura de voz esté activo ; e integrar mecanismos que garanticen que el asistente de notas se desconecta fehacientemente al concluir la sesión, impidiendo la captación accidental de conversaciones privadas posteriores .

9.5. Fase 4: El AI Verification Log como estándar deontológico

Para garantizar la responsabilidad proactiva y cumplir con el deber de competencia técnica [5,13], el despacho debe institucionalizar procedimientos de verificación humana obligatoria [7]. La única vía para evitar las sanciones por "alucinaciones" judiciales es la creación de un registro narrativo de auditoría interna: el *AI Verification Log* [23]. Este documento debe acompañar a cada entregable asistido por IA y detallar: la herramienta autorizada empleada y la versión del modelo; el historial de instrucciones (*prompts*) formuladas; y la declaración firmada del abogado confirmando que ha leído íntegramente cada fuente citada y ha contrastado la exactitud semántica de la transcripción de la reunión con el audio original [19,21].

9.6. Alfabetización en IA y cultura del riesgo (artículo 4 RIA)

La medida de gobernanza más eficaz es la inversión en el capital humano [13]. El artículo 4 del RIA impone a los despachos el deber legal de garantizar la alfabetización en IA de su personal [22]. Esta capacitación no debe ser un curso único, sino un programa de formación continua y actualizada ante la evolución mensual de los sistemas . La formación debe orientarse a que el abogado adquiera una "reserva de humanidad" reforzada, comprendiendo los fundamentos técnicos básicos para detectar sesgos algorítmicos o fallos en la lógica de los asistentes virtuales [21]. Solo desde una colaboración interdisciplinar entre juristas, tecnólogos y expertos en cumplimiento podrá consolidarse una integración de la IA que no debilite el Derecho, sino que lo refuerce .

9.7. Conclusión de la sección: El Compliance como ventaja competitiva

Las estrategias de *compliance* preventivo transforman la gestión del riesgo de una carga operativa en una ventaja competitiva [11,3]. Un despacho que puede demostrar mediante telemetría y bitácoras de verificación que mantiene una soberanía operativa real sobre el dato del cliente se sitúa en una posición de confianza superior en el mercado [3,11]. La gobernanza de la IA no consiste en detener la tecnología, sino en asegurar que cada palabra transcrita por una máquina permanezca bajo el control absoluto y el secreto profesional del abogado [12].

10. Conclusiones y recomendaciones operativas

10.1. El ocaso de la abogacía reactiva frente a la sombra tecnológica

El análisis desarrollado a lo largo de este artículo permite concluir que la abogacía se encuentra en una encrucijada histórica. No se trata de un mero cambio de herramientas, sino de una redefinición estructural de la infraestructura misma del Derecho [13]. La transición de la fase de experimentación a la de adopción estructural ha concluido: la inmensa mayoría de los juristas ya integra la inteligencia artificial en su núcleo operativo . Sin embargo, esta celeridad ha generado una brecha de gobernanza (*governance lag*) que ha propiciado el fenómeno del *Shadow AI* [2]. El uso no autorizado de herramientas de transcripción automática y asistentes de notas no es una práctica marginal, sino una respuesta sistémica de los profesionales ante la presión por la eficiencia y el ahorro de tiempo . El problema no reside en la tecnología *per se*, sino en la pérdida de la "soberanía operativa" sobre el dato del cliente [11,12].

10.2. Síntesis de hallazgos críticos

A partir de la investigación realizada, cabe sistematizar las siguientes conclusiones fundamentales:

Primera conclusión: vulneración irreversible del secreto profesional. El uso de transcriptores de consumo público asimila la práctica profesional al acto negligente de abandonar expedientes en espacios públicos [14]. Una vez que los datos de voz salen de la esfera de control de la firma hacia modelos cuyos términos de servicio autorizan el reentrenamiento, el privilegio abogado-cliente se rompe de forma irreversible [16], exponiéndose la estrategia de defensa a futuras exhibiciones de prueba en litigios [7].

Segunda conclusión: infracciones sistémicas al RGPD. La firma legal asume plenamente la condición de responsable del tratamiento en el uso de estas herramientas [19]. El *Shadow AI* anula el cumplimiento del principio de responsabilidad proactiva (*accountability*), impide la realización de evaluaciones de impacto y vulnera el principio de exactitud por las "alucinaciones" acústicas de los modelos probabilísticos [20].

Tercera conclusión: imperativo legal bajo el RIA. El Reglamento (UE) 2024/1689 eleva la gobernanza de la IA a un requisito legal ineludible [22]. El deber de alfabetización (artículo 4) y la exigencia de supervisión humana efectiva (artículo 14) obligan a los despachos a sustituir las herramientas en la sombra por marcos de observabilidad técnica que permitan demostrar el control humano sobre cada resultado [3]. El artículo 99 del RIA establece un régimen sancionador cuyas

cuantías máximas alcanzan los 35 millones de euros o el 7% del volumen de negocio anual global .

Cuarta conclusión: responsabilidad y seguros. El mercado asegurador de responsabilidad civil profesional está incorporando cláusulas de exclusión para incidentes derivados de "IA no auditada" [11]. La falta de capacitación técnica del abogado que usa un asistente clandestino puede ser calificada como "culpa grave", dejando a la firma sin cobertura ante una brecha de datos o un error procesal derivado de una mala transcripción [13,17].

10.3. Hoja de ruta para una gobernanza proactiva (Checklist operativo)

Para mitigar los riesgos identificados y garantizar una transición segura hacia la era de la IA, se propone la siguiente hoja de ruta estratégica, estructurada en cuatro niveles de control [5,13,23]. El presente checklist tiene carácter propositivo y no sustituye al asesoramiento legal personalizado adaptado a las circunstancias concretas de cada firma.

Nivel 1: Gobernanza y Estructura Organizativa

Política Corporativa de IA (BYOAI): redactar y difundir una política interna que delimite qué herramientas están autorizadas, para qué fines y por qué perfiles profesionales [23]. Inventario de Activos de IA: mantener un registro exhaustivo y actualizado de todos los sistemas de IA utilizados en la firma, documentando su nivel de riesgo bajo el RIA [11,22]. Canal de Solicitudes Ágil: articular un procedimiento para que los abogados propongan nuevas herramientas útiles, evitando que la frustración operativa derive en el uso de transcriptores personales [7,13].

Nivel 2: Seguridad Técnica y Observabilidad

Telemetría y Descubrimiento Activo: articular herramientas de monitorización de red capaces de detectar llamadas a APIs de IA no autorizadas [3,7]. Modalidad *Enterprise* Obligatoria: contratar exclusivamente licencias corporativas con cláusulas de "no-reutilización de datos" y residencia en el EEE [10,18]. Entornos Seguros (*Sandboxes*): proveer a los asociados de entornos de experimentación locales donde puedan probar modelos de lenguaje sin riesgo de filtración hacia nubes públicas [13,15].

Nivel 3: Protocolo en Reuniones con Clientes

Transparencia Reforzada: configurar indicadores visuales ininterrumpidos en las plataformas de videoconferencia que informen de que el asistente de notas está activo [19]. Consentimiento Específico: utilizar plantillas informativas que aclaren los riesgos del procesamiento por IA y aseguren la desactivación automática del canal de grabación al concluir la sesión [20]. Revisión Humana Sistemática: prohibir

la incorporación de transcripciones generadas por IA a expedientes oficiales sin un proceso de validación cruzada con el audio original [21,22].

Nivel 4: Formación y Ética (Reserva de Humanidad)

Programa de Alfabetización en IA: cumplir con el artículo 4 del RIA mediante formación continua sobre los fundamentos técnicos, los riesgos de sesgo y las limitaciones de la IA generativa [13,22]. *AI Verification Log*: institucionalizar la creación de bitácoras de auditoría interna que documenten qué IA se usó en cada entregable y qué medidas de verificación humana se llevaron a cabo [7,23]. Cultura de Responsabilidad: fomentar un entorno donde el abogado sea consciente de que la tecnología es un colaborador infraestructural, pero la responsabilidad ética y legal sigue siendo personal e indelegable [5,12].

10.4. Recomendación estratégica final: El Compliance como ventaja competitiva

El cumplimiento normativo en materia de IA no debe percibirse como un obstáculo a la innovación, sino como la mayor ventaja competitiva que un despacho puede ofrecer en el mercado jurídico actual [11,3]. En un entorno saturado de automatización genérica, la "soberanía operativa" y la garantía técnica del secreto profesional serán los activos diferenciales que permitan a las firmas líderes distinguirse [3,11].

La "reserva de humanidad" es el límite infranqueable de la abogacía algorítmica [13,21]. Un despacho que puede demostrar mediante registros de auditoría y telemetría que mantiene el control humano sobre cada palabra transcrita por una máquina, no solo cumple con el RIA y el RGPD, sino que refuerza el contrato de confianza fundamental que sostiene el Estado de Derecho [22]. La respuesta al desafío del *Shadow AI* no es la prohibición nostálgica, sino la arquitectura de un entorno de diseño seguro donde la eficiencia tecnológica y la ética profesional operen en absoluta simbiosis [3].

11. Referencias bibliográficas

1. WOLTERS KLUWER, Informe de la Encuesta Future Ready Lawyer 2026: Construyendo confianza en la era de la inteligencia artificial. Alphen aan den Rijn: Wolters Kluwer Legal & Regulatory, 2026. Disponible en: https://www.wolterskluwer.com/es-es/know/future-ready-lawyer-2026 [consulta: 11/06/2026].

2. FEITO, Alicia y MIOT, Grégoire, "El informe Future Ready Lawyer es definitivo: el 92% de los juristas ya usa IA y la fase de experimentación ha terminado", Confilegal, 20 de abril de 2026. Disponible en: https://confilegal.com/20260420-el-informe-future-ready-lawyer-confirma-la-integracion-de-la-ia-en-el-sector/ [consulta: 11/06/2026].

3. BANDARA, Eranga et al., "AI Trust OS — A Continuous Governance Framework for Autonomous AI Observability and Zero-Trust Compliance in Enterprise Environments", arXiv preprint arXiv:2604.04749v1, 6 de abril de 2026. DOI: https://doi.org/10.48550/arXiv.2604.04749. [Preprint; no revisado por pares.]

4. AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS (AEPD), "Transcripción de voz con IA (II): responsabilidad, derechos y transparencia", Blog de Innovación y Tecnología, 20 de abril de 2026. Disponible en: https://www.aepd.es/prensa-y-comunicacion/blog/transcripcion-de-voz-con-ia-ii [consulta: 11/06/2026].

5. CONSEJO GENERAL DE LA ABOGACÍA ESPAÑOLA (CGAE), Circular 3/2026 del Pleno del CGAE sobre el uso de herramientas de inteligencia artificial generativa en la elaboración de textos profesionales y defensa jurídica. Madrid: CGAE, 10 de abril de 2026.

6. ILUSTRE COLEGIO DE LA ABOGACÍA DE MADRID (ICAM), Guía de Buenas Prácticas para el Uso de la Inteligencia Artificial en la Abogacía. Madrid: ICAM, 2026, coord. Mabel Klimt. Disponible en: https://web.icam.es/el-icam-lanza-la-primera-guia-practica-para-un-uso-responsable-de-la-ia-en-la-abogacia/ [consulta: 11/06/2026].

7. Síntesis analítica del conjunto de fuentes primarias citadas en el presente artículo, elaborada mediante contraste sistemático entre la normativa vigente (RGPD, RIA, LO 5/2024), las directrices de las autoridades de control (AEPD, CGAE) y la literatura técnico-jurídica especializada referenciada en los apartados correspondientes.

8. SILIC, M., SILIC, D. y KIND-TRÜLLER, K., "From shadow IT to shadow AI—threats, risks and opportunities for organizations", Strategic Change, 2025. DOI: https://doi.org/10.1002/jsc.2682.

9. AUTOR COLECTIVO, "From Frontier to Shadow AI: A Simmering Threat to Assurance and Security in Critical Infrastructure", arXiv preprint arXiv:2606.00088v1, junio de 2026. Disponible en: https://arxiv.org/html/2606.00088v1 [consulta: 11/06/2026]. [Preprint; no revisado por pares.]

10. AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS (AEPD), Resumen básico de obligaciones y recomendaciones para la gestión de IAG en la AEPD. Madrid: AEPD, División de Innovación y Tecnología, enero de 2026. Disponible en: https://www.aepd.es/guias/sumario-recomendaciones-iag-aepd.pdf [consulta: 11/06/2026].

11. WOLTERS KLUWER, "Seguridad de la información: un nuevo riesgo omnipresente en el sector jurídico", Expert Insights, 10 de marzo de 2026. Disponible en: https://www.wolterskluwer.com/es-es/expert-insights/seguridad-informacion-rgpd-privacidad-datos-amenazas-ciberneticas-legal [consulta: 11/06/2026].

12. Ley Orgánica 5/2024, de 11 de noviembre, del Derecho de Defensa, BOE núm. 273, de 12 de noviembre de 2024. Referencia BOE-A-2024-23422.

13. CONSEJO GENERAL DE LA ABOGACÍA ESPAÑOLA (CGAE) e ILUSTRE COLEGIO DE ABOGADOS DE VALENCIA (ICAV), Libro Blanco sobre Inteligencia Artificial y Abogacía. Madrid/Valencia: CGAE-ICAV, enero de 2026. Disponible en: https://www.abogacia.es/wp-content/uploads/2026/01/libro-ai-digital.pdf [consulta: 11/06/2026].

14. AMERICAN BAR ASSOCIATION (ABA), "Why You Need an AI Policy Yesterday, and How to Write It", Law Practice Magazine, vol. 52, núm. 2, marzo-abril 2026. Disponible en: https://www.americanbar.org/groups/law_practice/resources/law-practice-magazine/2026/march-april-2026/ [consulta: 11/06/2026].

15. AMERICAN BAR ASSOCIATION (ABA), "Navigating Today's AI Landscape with an Ethical Polestar", SciTech Lawyer, vol. 18, núm. 3, primavera de 2026. Disponible en: https://www.americanbar.org/groups/science_technology/resources/scitech-lawyer/2026-spring/ [consulta: 11/06/2026].

16. CONSEJO GENERAL DE LA ABOGACÍA ESPAÑOLA (CGAE), Circular 1/2025 del Pleno del CGAE sobre protección del Secreto Profesional en entornos digitales y servicios de computación en la nube. Madrid: CGAE, noviembre de 2025.

17. HOMOKI, P., Guide on the use of Artificial Intelligence-based tools by lawyers and law firms in the EU. Bruselas: Council of Bars and Law Societies of Europe (CCBE) y European Lawyers Foundation, 2022. Disponible en: https://www.ccbe.eu/fileadmin/speciality_distribution/public/documents/IT_LAW/ITL_Reports_studies/EN_ITL_20220331_Guide-AI4L.pdf [consulta: 11/06/2026].

18. AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS (AEPD), "Soberanía operativa en tratamientos de datos personales", Nota Técnica de la División de Innovación y Tecnología, febrero de 2026. Disponible en: https://www.aepd.es/areas-de-actuacion/innovacion-y-tecnologia [consulta: 11/06/2026].

19. AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS (AEPD), "Transcripción de voz con IA: implicaciones para la protección de datos", Blog de Innovación y Tecnología, 14 de enero de 2026. Disponible en: https://www.aepd.es/prensa-y-comunicacion/blog/transcripcion-de-voz-con-ia [consulta: 11/06/2026].

20. AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS (AEPD), "Inteligencia Artificial Agéntica desde la perspectiva de Protección de Datos", Nota Técnica, febrero de 2026. Disponible en: https://www.aepd.es/prensa-y-comunicacion/blog/orientaciones-aepd-ia-agentica [consulta: 11/06/2026].

21. CONSEJO GENERAL DEL PODER JUDICIAL (CGPJ), Resumen de la Instrucción 2/2026 sobre la utilización de sistemas de inteligencia artificial en el ejercicio de la actividad jurisdiccional. Madrid: CGPJ, enero de 2026. Ponente: Joaquín Delgado Martín. Disponible en:

https://www.abogacia.es/wp-content/uploads/2026/02/NOTAS-RESUMEN-DE-LA-INCTRUCCION-2-26-IA-EN-LA-FUNCION-JURISDICCIONAL.pdf [consulta: 11/06/2026].

22. Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, de 13 de junio de 2024, por el que se establecen normas armonizadas en materia de inteligencia artificial [en adelante, RIA], DO L 2024/1689, de 12 de julio de 2024. Disponible en: http://data.europa.eu/eli/reg/2024/1689/oj.

23. AMERICAN BAR ASSOCIATION (ABA), "AI in the Trenches and on the Bench", Business Law Today, 8 de abril de 2026. Disponible en: https://www.americanbar.org/groups/business_law/resources/business-law-today/2026-april/ai-in-trenches-and-on-bench/ [consulta: 11/06/2026].

24. CONSEJO DE EUROPA, Convenio Marco sobre Inteligencia Artificial y Derechos Humanos, Democracia y Estado de Derecho (CETS núm. 225), abierto a la firma en Vilnius el 5 de septiembre de 2024. Primer tratado internacional jurídicamente vinculante sobre IA. Disponible en: https://www.coe.int/en/web/artificial-intelligence/the-framework-convention-on-ai [consulta: 11/06/2026].