EL *LEGAL DESIGN* COMO ELEMENTO ESTRUCTURAL EN LA DEFINICIÓN DE LA POLÍTICA DE GOBERNANZA DEL USO DE LA INTELIGENCIA ARTIFICIAL EN LAS ORGANIZACIONES

I. PLANTEAMIENTO DEL PROBLEMA Y FUNDAMENTACIÓN TEÓRICA

La incorporación progresiva de sistemas de Inteligencia Artificial (IA) en el tejido organizativo contemporáneo ha trascendido la esfera meramente tecnológica para convertirse en un fenómeno que redefine los paradigmas tradicionales de gestión del riesgo jurídico, cumplimiento normativo y arquitectura de la responsabilidad corporativa. Esta transformación estructural ha encontrado su cristalización normativa en el 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, *AI Act*[1]).

El legislador europeo ha optado por un modelo regulatorio sofisticado, basado en la estratificación del riesgo, la exigibilidad de trazabilidad operativa y la institucionalización de mecanismos efectivos de rendición de cuentas. Sin embargo, la experiencia acumulada tras más de cinco años de aplicación del Reglamento General de Protección de Datos (RGPD) evidencia una realidad ineludible: la existencia de marcos normativos técnicamente solventes no garantiza, per se, su implementación organizativa efectiva.

La hipótesis central que articula este trabajo sostiene que la definición de políticas de gobernanza del uso de la IA que no incorporen metodologías estructuradas de *legal design* está destinada al fracaso desde una triple perspectiva: cumplimiento normativo sustantivo, prevención efectiva de riesgos jurídicos y consolidación de una cultura organizativa coherente con las exigencias regulatorias.

El *legal design*, en este contexto, trasciende su concepción tradicional como herramienta de comunicación jurídica para configurarse como instrumento estructural de ingeniería organizativa. Su aplicación debe materializarse de forma transversal en los procesos de evaluación de riesgos, definición de procedimientos internos, elaboración de políticas corporativas, estructuración de sistemas documentales, diseño de programas formativos y articulación de las interfaces con usuarios y terceros.

[1] Primer marco jurídico integral sobre inteligencia artificial en el mundo, impulsado por la Unión Europea. Su objetivo es regular la tecnología para garantizar que sea segura, ética y respete los derechos fundamentales.

II. MARCO NORMATIVO APLICABLE: DE LA FRAGMENTACIÓN REGULATORIA A LA INTEGRACIÓN SISTEMÁTICA

1. El *AI Act* como paradigma de regulación basada en el riesgo

El *AI Act* inaugura un modelo regulatorio que abandona los enfoques binarios tradicionales (permitido/prohibido) para adoptar una aproximación graduada basada en la evaluación diferenciada del riesgo. La arquitectura normativa establece cuatro categorías fundamentales: sistemas de riesgo inaceptable, sistemas de alto riesgo, sistemas sujetos a obligaciones de transparencia específicas, y sistemas de riesgo mínimo.

Para los sistemas clasificados como de alto riesgo, el Reglamento no es un mero marco de cumplimiento estático; por el contrario, obliga a las organizaciones a guiar una arquitectura de control interno real, movilizando recursos y procesos que hasta ahora eran opcionales:

- Sistema integral de gestión de riesgos, no basta con una "foto fija"; se exige un control dinámico que cubra todo el ciclo de vida.

- El foco se desplaza hacia protocolos estrictos de entrenamiento, validación y testeo.

- El expediente técnico[2] como prueba: La conformidad ya no es una intención, sino que requiere documentación exhaustiva y auditable.

- Se impone la automatización de los *logs*[3] para reconstruir fielmente la operativa en cualquier momento.

- El deber de información se intensifica para que se comprendan capacidades y límites reales.

- Más allá de un "botón de pánico", se requieren mecanismos de control efectivo sobre el algoritmo, esto quiere decir que la supervisión no puede ser un trámite meramente formal o reactivo. Al contrario, exige que el responsable humano tenga la formación técnica y la autoridad jerárquica necesarias para entrar en el sistema, interpretar sus sesgos en tiempo

[2] Documentación integral y auditable que compendia los cálculos, procedimientos y validaciones técnicas de una obra o servicio. Su función es transformar la presunción de cumplimiento en una certeza documental verificable ante terceros o autoridades regulatorias.

[3] Archivos de registro que actúan como la "caja negra" del sistema de IA. Almacenan de forma sistemática cada acción u omisión del algoritmo, permitiendo reconstruir ex post cualquier incidente o decisión técnica relevante.

real y, si fuera necesario, neutralizar una decisión automatizada antes de que produzca efectos jurídicos lesivos.

En definitiva, el blindaje técnico —exactitud, robustez y ciberseguridad— deja de ser un ideal para convertirse en una garantía exigible por diseño.

Lo que este entramado normativo rechaza de plano es el cumplimiento "de fachada", el Reglamento exige, por el contrario, la construcción de procesos internos genuinamente comprensibles, la estructuración sistemática de la documentación corporativa, el desarrollo de protocolos operativos claros y funcionales, y la asignación inequívoca de responsabilidades organizativas.

2. La interconexión sistemática con el RGPD: accountability y privacy by design

La normativa sobre IA no debe entenderse como un compartimento aislado; al contrario, se entrelaza de forma orgánica con el ecosistema de protección de datos ya consolidado en Europa. Esta simbiosis normativa cobra especial relevancia en cinco áreas críticas:

Los principios generales del tratamiento (art. 5 RGPD), particularmente los de licitud, lealtad, transparencia, limitación de la finalidad, minimización de datos, exactitud, limitación del plazo de conservación, integridad, confidencialidad y responsabilidad proactiva, adquieren una dimensión específica cuando se aplican a sistemas automatizados de toma de decisiones.

El principio de responsabilidad proactiva (art. 24 RGPD) impone al responsable del tratamiento la obligación de aplicar medidas técnicas y organizativas apropiadas para garantizar y poder demostrar que el tratamiento se realiza conforme al Reglamento. Este principio encuentra un desarrollo natural en las obligaciones de gobernanza del *AI Act*.

El paradigma de protección de datos desde el diseño y por defecto (art. 25 RGPD) constituye el antecedente normativo directo del enfoque preventivo que caracteriza al *AI Act*. Ambos instrumentos comparten la filosofía de integración de las garantías jurídicas en la propia arquitectura técnica de los sistemas.

Las evaluaciones de impacto en materia de protección de datos (art. 35 del RGPD) sirven como precedente metodológico para las evaluaciones de riesgo requeridas por el *AI Act*, particularmente cuando los tratamientos incluyen decisiones automatizadas que generan efectos jurídicos o influyen de manera significativa en los derechos y la vida de las personas afectadas.

El derecho específico a no ser objeto de decisiones basadas únicamente en el tratamiento automatizado (art. 22 RGPD) establece el marco de garantías individuales que debe complementarse con las obligaciones organizativas del *AI Act.*

3. Dimensión nacional: responsabilidad civil y penal derivada del uso de sistemas de IA

En el marco del ordenamiento jurídico español, el uso incorrecto de sistemas de inteligencia artificial puede dar lugar a la aplicación de diversos regímenes de responsabilidad, los cuales deben ser anticipados y gestionados de forma preventiva mediante políticas de gobernanza adecuadas.

En el ámbito de la responsabilidad civil extracontractual, el art. 1902 del Código Civil establece el marco general para la exigencia de responsabilidad por daños causados por acción u omisión en que intervenga cualquier género de culpa o negligencia. La jurisprudencia del Tribunal Supremo ha consolidado una doctrina que exige la concurrencia de acción u omisión imputable al demandado, daño o perjuicio causado a la víctima, y relación de causalidad entre ambos elementos.

La Directiva (UE) 2024/2853, que sustituye a la Directiva 85/374/CEE sobre responsabilidad por productos defectuosos, incorpora expresamente determinados elementos de software y sistemas digitales en su ámbito de aplicación, lo que tendrá una incidencia directa en la exigibilidad de responsabilidad por sistemas de IA defectuosos.

Finalmente, en el plano penal, el Art. 31 bis del Código Penal sitúa la gobernanza de la IA en el centro de la estrategia de defensa corporativa. Bajo este precepto, la responsabilidad penal de las personas jurídicas no es una fatalidad inevitable, sino que puede mitigarse o incluso exonerarse mediante la implementación de modelos de organización y gestión eficaces. En este sentido, la vigilancia y el control sobre los algoritmos dejan de ser una opción técnica para configurarse como una pieza esencial del *compliance*: solo aquel modelo que demuestre una supervisión real y apta para prevenir delitos podrá actuar como un escudo legal efectivo para la organización.

III. FUNDAMENTACIÓN TEÓRICA Y METODOLÓGICA DEL LEGAL DESIGN

1. Origen conceptual y desarrollo académico

El *legal design* emerge en el ecosistema académico anglosajón como respuesta a la creciente desconexión entre la sofisticación técnica del derecho y su operatividad práctica. Margaret Hagan, desde el Stanford Legal Design Lab, establece un cambio de paradigma radical: el derecho no se valida por su sofisticación doctrinal, sino por su utilidad para el destinatario final. Bajo esta premisa, la norma debe ser diseñada "por y para" el usuario, convirtiendo la claridad en un requisito de validez práctica.

Helena Haapio y Stefania Passera han desarrollado el concepto de "contratos como interfaces"[3], defendiendo que los instrumentos jurídicos constituyen verdaderas interfaces de comunicación que deben optimizarse para facilitar la comprensión, la toma de decisiones y el cumplimiento por parte de usuarios con diferentes niveles de especialización jurídica.

Tim Brown, desde la perspectiva del design thinking[4] corporativo, ha proporcionado el marco metodológico general que el *legal design* adapta al ámbito jurídico. Este marco se articula en torno a cinco principios fundamentales: enfoque centrado en el usuario, que prioriza las necesidades y limitaciones de quienes deben aplicar efectivamente las normas; metodología de prototipado, que permite la validación iterativa de soluciones; procesos de iteración sistemática, que facilitan la mejora continua; técnicas de visualización, que traducen conceptos abstractos en representaciones comprensibles; y aproximación interdisciplinaria, que integra competencias jurídicas, tecnológicas y organizativas.

2. Aplicación específica a la gobernanza de sistemas de IA

En el contexto específico de la gobernanza de IA, el *legal design* debe orientarse hacia múltiples usuarios internos, cada uno con necesidades informativas y operativas diferentes: los responsables técnicos del desarrollo y mantenimiento de sistemas, que necesitan traducciones precisas de las obligaciones jurídicas en las especificaciones

[4] Marco de trabajo interdisciplinar que prioriza la experiencia del usuario final en la creación de soluciones. A diferencia de los métodos analíticos tradicionales, el *design thinking* utiliza un pensamiento divergente y procesos iterativos para asegurar que la solución propuesta sea, ante todo, funcional y comprensible para quienes deben interactuar con ella.

técnicas; los órganos de cumplimiento normativo, que necesitan herramientas de monitorización y control; los órganos de administración y dirección, que demandan información sintética para la toma de decisiones estratégicas; y los supervisores humanos de los sistemas, que deben disponer de interfaces y protocolos claros para el ejercicio efectivo de sus funciones.

IV. IMPLEMENTACIÓN PRÁCTICA DEL LEGAL DESIGN EN POLÍTICAS DE GOBERNANZA DE IA

1. Metodología de mapeo normativo visual

El punto de partida para una gobernanza de IA que pretenda ser operativa, radica en lo que podríamos denominar, el mapa de obligaciones. Este primer estadio exige trascender la lectura lineal de la norma para acometer una visualización sistemática de todo el ecosistema regulatorio que rodea al algoritmo. No se trata simplemente de enumerar leyes, sino de entender cómo colisionan y se complementan en el día a día de la organización.

Este mapeo integral debe desplegarse, al menos, en cuatro niveles críticos:

1. El núcleo duro del cumplimiento: La convergencia obligatoria entre el *AI Act* y el RGPD, donde se definen los parámetros de riesgo y las salvaguardas de privacidad que actúan como la constitución técnica del sistema.
2. La especificidad sectorial: El análisis no puede ser genérico; debe aterrizar en las normativas propias del sector (financiero, sanitario, seguros, etc.), donde las exigencias de transparencia y solvencia suelen ser más granulares y restrictivas.
3. El factor humano y laboral: Es imperativo integrar la regulación laboral vigente que supervisa la gestión de recursos humanos mediante algoritmos. En este punto, el *Legal Design* debe clarificar los derechos de información de los representantes de los trabajadores frente a la toma de decisiones automatizada, evitando que la tecnología impida la visión y la toma en cuenta de los derechos fundamentales en el empleo.
4. La protección del consumidor final: Cuando el sistema interactúa con personas físicas, entran en juego los marcos de protección al consumidor y las normativas sobre competencia desleal. Aquí, la visualización sistemática permite prever

riesgos de sesgos comerciales o falta de transparencia en la contratación algorítmica.

El resultado de este mapeo debe materializarse en instrumentos visuales que faciliten la detección de lagunas regulatorias, la identificación de solapamientos normativos, y la priorización de obligaciones según su impacto en el riesgo organizativo. Las técnicas de visualización pueden incluir mapas de obligaciones estructurados por ámbitos normativos.

En última instancia, el uso de diagramas de flujo secuenciales[5] permite que cada departamento sepa exactamente qué obligación le corresponde cumplir en cada fase del ciclo de vida de la IA, desde el diseño del modelo hasta su puesta en producción.

2. Diseño organizativo de roles y responsabilidades

La gobernanza efectiva de la IA exige la definición precisa y la asignación inequívoca de responsabilidades organizativas. El *legal design* facilita esta tarea mediante la elaboración de organigramas funcionales que identifiquen claramente al responsable general del sistema de IA, al responsable técnico del desarrollo y mantenimiento, al responsable de cumplimiento normativo, y al comité de IA cuando su constitución resulte necesaria.

Estos organigramas deben complementarse con flujos de decisión escalonados que especifiquen los procedimientos de toma de decisiones en situaciones ordinarias y extraordinarias, y con protocolos de activación ante incidencias que definan las cadenas de responsabilidad y los plazos de actuación cuando se detecten disfunciones en los sistemas.

Debemos considerar lo anterior como algo esencial en el desarrollo de un buen sistema de gobernanza de la IA, las compañías deben asignar de manera correcta los perfiles de los responsables, teniendo estos una buena capacitación técnica para saber detectar un sistema defectuoso y asegurarse de cumplir con la norma en la toma de decisiones, no porque una decisión sea más beneficiosa siempre es acorde con la normativa.

3. La supervisión humana efectiva

El art. 14 del *AI Act* dice, en su apartado uno: *"1. Los sistemas de IA de alto riesgo se diseñarán y desarrollarán de tal manera, incluso con herramientas adecuadas de interfaz*

[5] Representaciones gráficas que esquematizan la cronología de acciones, decisiones y controles dentro de un proceso.

persona-máquina, que puedan ser supervisados eficazmente por personas físicas durante el período en que estén en uso". Esta exigencia normativa trasciende la mera declaración formal de la existencia de supervisión humana para demandar la configuración efectiva de las condiciones que hagan posible dicha supervisión.

Llegados a este punto, la cuestión fundamental que deben resolver las organizaciones no es qué dice la norma, sino cómo se ejecuta: *¿Cómo podemos/debemos transformar el mandato genérico de "supervisión humana" en una capacidad real de intervención técnica y jurídica?*

El *legal design* permite traducir esta obligación abstracta en especificaciones operativas concretas: identificación nominal de las personas responsables de la supervisión, definición temporal de los momentos en que debe ejercerse la supervisión, especificación informativa de los datos y alertas que deben ponerse a disposición del supervisor humano, y delimitación competencial de la capacidad de intervención del supervisor sobre el funcionamiento del sistema.

4. Estructuración de la documentación técnica y garantía de trazabilidad

El art. 11 del *AI Act* impone a los proveedores de sistemas de alto riesgo la obligación de elaborar documentación técnica antes de que dichos sistemas se pongan en el mercado o se pongan en servicio. Esta documentación debe permitir la evaluación de la conformidad del sistema de IA con los requisitos establecidos y debe contener la información necesaria para que las autoridades de supervisión y los organismos notificados puedan cumplir sus funciones.

Desde una perspectiva probatoria, esta documentación constituirá el elemento central en procedimientos de inspección administrativa, procesos sancionadores, y litigios civiles derivados del funcionamiento defectuoso de sistemas de IA. El *legal design* permite estructurar esta documentación mediante aproximaciones por capas que faciliten el acceso diferenciado según el perfil del usuario: nivel ejecutivo, con resúmenes sintéticos orientados a la toma de decisiones estratégicas; nivel jurídico, con desarrollo detallado de las medidas de cumplimiento adoptadas; y nivel técnico, con especificaciones completas del funcionamiento del sistema.

V. ANÁLISIS DE DERECHO COMPARADO: MODELOS DE GOBERNANZA EN JURISDICCIONES RELEVANTES

1. Estados Unidos: el modelo federal descentralizado

El ordenamiento jurídico estadounidense carece de una regulación federal específica equivalente al *AI Act* europeo. Sin embargo, se han desarrollado instrumentos normativos y marcos de orientación que resultan relevantes para el análisis comparado.

El NIST AI Risk Management Framework, publicado en enero de 2023, establece un marco voluntario estructurado en torno a cuatro funciones organizativas: Govern (Gobernar), que se centra en el establecimiento de políticas y la supervisión organizativa; Map (Mapear), orientada a la identificación y categorización de riesgos; Measure (Medir), que desarrolla metodologías de análisis y evaluación; y Manage (Gestionar), que implementa respuestas específicas a los riesgos identificados.

La Executive Order 14110[6], anulada por el gobierno actual de los Estados Unidos, fue promulgada el 30 de octubre de 2023, y supuso un giro hacia la codificación de la confianza. Lejos de ser un mero protocolo administrativo, esta orden establecía un estándar de rigor para el despliegue de IA en el ámbito federal, forzando una convergencia entre la seguridad nacional y la ética técnica que redefinía las reglas de juego para cualquier desarrollador que colaborase con la administración estadounidense.

Sin embargo, tras la corta vigencia de la norma, el escenario estadounidense ha experimentado una mutación radical con el cambio de administración en 2025. La Executive Order 14110 fue revocada y sustituida por la Executive Order 14179[7], en enero de 2025, bajo la premisa de "eliminar las barreras al liderazgo tecnológico de Estados Unidos". Esta transición marca un alejamiento del enfoque preventivo europeo para abrazar una doctrina de desregulación competitiva. Donde la orden anterior ponía el foco

[6] Executive Order 14110 ("Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence"): Orden presidencial emitida el 30 de octubre de 2023 que constituyó el primer marco federal integral de EE. UU. para la gobernanza de la IA. Establecía mandatos sobre seguridad nacional, protección de la privacidad y pruebas de seguridad obligatorias (*red-teaming*) para modelos de gran escala. Fue revocada el 20 de enero de 2025 y sustituida por la EO 14179, la cual eliminó la mayoría de sus controles de cumplimiento en favor de un modelo de desregulación competitiva.

[7] Executive Order 14179 ("Removing Barriers to American Leadership in AI"): Disposición presidencial de enero de 2025 que revoca la normativa anterior (EO 14110). Su objetivo primordial es simplificar el despliegue de la IA mediante la eliminación de cargas administrativas y controles federales de seguridad, bajo la premisa de asegurar la hegemonía tecnológica de Estados Unidos frente a competidores estratégicos.

en la seguridad nacional y la mitigación de riesgos, el marco actual prioriza la aceleración del despliegue algorítmico y la eliminación de cargas burocráticas.

Para las organizaciones, este giro ha creado un paradigma de cumplimiento asimétrico: mientras la Unión Europea consolida el *AI Act*, Estados Unidos desmantela sus controles federales, dejando a las empresas ante un mosaico de leyes estatales que la administración federal intenta impugnar activamente. En este contexto de inestabilidad normativa, el *Legal Design* deja de ser una opción de claridad para convertirse en una herramienta de supervivencia, permitiendo a las compañías modular sus políticas de gobernanza según la jurisdicción sin perder la coherencia operativa.

2. Reino Unido: principios regulatorios y descentralización sectorial

El "AI Regulation White Paper"[8], publicado en marzo de 2023, articula la aproximación británica en torno a cinco principios regulatorios fundamentales: seguridad, transparencia, equidad, rendición de cuentas, y contestabilidad y reparación. Este modelo se caracteriza por su aplicación descentralizada a través de los reguladores sectoriales existentes.

La descentralización normativa obliga a las organizaciones a diseñar marcos de gobernanza interna que integren coherentemente las orientaciones de múltiples autoridades sectoriales, lo que refuerza la necesidad de metodologías *de legal design* para la armonización de obligaciones potencialmente divergentes.

4. Francia y Alemania: integración con marcos éticos preexistentes

La Commission Nationale de l'Informatique et des Libertés[9] (CNIL) francesa ha desarrollado orientaciones específicas sobre IA y protección de datos que enfatizan la necesidad de evaluaciones de impacto estructuradas y la implementación de sistemas de gobernanza graduados según el nivel de riesgo.Alemania, a través de la Data Ethics

[8] Documento estratégico publicado por el Gobierno del Reino Unido en marzo de 2023 que define una aproximación regulatoria a la IA basada en principios, no en leyes rígidas. Su característica principal es la delegación de la supervisión en los organismos reguladores ya existentes, permitiendo una adaptación sectorial específica frente a la creación de un marco normativo centralizado.

[9] Commission Nationale de l'Informatique et des Libertés (CNIL): Autoridad administrativa independiente de Francia encargada de velar por la protección de datos personales.

Commission[10] constituida en 2018, ha elaborado recomendaciones que subrayan la importancia de sistemas de gobernanza diferenciados según el ámbito de aplicación y el impacto potencial de los sistemas algorítmicos.

VI. El *abogado* como arquitecto de gobernanza: evolución del rol profesional

La llegada de la inteligencia artificial ha transformado las reglas del juego para el mundo legal. Hoy ya no es suficiente con saber interpretar las leyes; el nuevo escenario exige que el abogado dé un paso al frente y participe directamente en cómo se diseña la tecnología. Debemos convertirnos en una especie de "traductor bilingüe" entre el lenguaje del derecho y el de la programación. Esto no significa que el abogado deba aprender a programar, sino que debe desarrollar la capacidad crítica para cuestionar la lógica del sistema. El objetivo es abrir esas "cajas negras" y asegurar que cualquier decisión automatizada no solo sea rápida, sino que pueda explicarse y defenderse con claridad ante un juez o un regulador. En definitiva, se trata de que el razonamiento jurídico no se pierda entre los procesos de la máquina.

En este entorno donde las normas aún se están definiendo, la gobernanza basada en el *legal design* deja de ser un simple trámite burocrático para convertirse en nuestra mejor defensa. El enfoque debe cambiar: la documentación y los controles deben nacer desde el primer minuto en que se diseña la herramienta. Esto nos permite estar siempre listos para un posible conflicto o litigio (*litigation readiness*). En el futuro, la solidez de una empresa no se demostrará recitando leyes, sino probando que sus soluciones inteligentes fueron creadas desde el origen para ser auditables, transparentes y honestas. Se trata de pasar del "cumplo porque me obligan" al "demuestro que soy responsable".

Finalmente, el abogado debe dejar de ser visto solo como un vigilante para convertirse en el guardián de la esencia de la empresa. El liderazgo jurídico actual consiste en garantizar que el uso de la IA no dañe la reputación de la entidad ni pase por encima de los derechos de las personas. Debemos entender que, si el motor del sistema falla éticamente, la organización entera pierde su integridad. En esta nueva etapa, nuestra misión es asegurar

[10] Data Ethics Commission (Alemania): Órgano consultivo independiente establecido por el Gobierno Federal alemán que en 2019 propuso el influyente modelo de "pirámide de riesgo crítica" para sistemas algorítmicos. Este enfoque de regulación escalonada, basado en la intensidad del daño potencial, constituye el precedente doctrinal directo de la clasificación de riesgos adoptada posteriormente por el Reglamento Europeo de IA.

que el éxito tecnológico nunca se consiga a costa de la confianza de la sociedad, convirtiendo la ética operativa en el activo más valioso de la compañía.

VII. CONCLUSIÓN

El análisis desarrollado a lo largo de este trabajo permite extraer una hoja de ruta clara para el jurista contemporáneo. El despliegue de la inteligencia artificial no es un fenómeno puramente técnico, sino un desafío normativo que redefine nuestra forma de entender la responsabilidad y el cumplimiento.

En primer lugar, debemos entender que el *AI Act* es estructural y no solo prohibitivo. No basta con "no incumplir"; la norma exige una proactividad constante. Los sistemas de alto riesgo nos obligan a pasar de un modelo de reacción a uno de prevención, donde la documentación, la transparencia y el control humano deben estar integrados en el código genético de cualquier herramienta inteligente que se despliegue en el mercado.

Esta exigencia jurídica tiene una vertiente probatoria fundamental. Como hemos visto, la jurisprudencia española ha dejado de conformarse con modelos de cumplimiento que solo existen en el papel. Siguiendo la estela de lo que nuestros tribunales exigen en materia de responsabilidad penal de las personas jurídicas, la gobernanza de la IA debe demostrar una eficacia real. En un futuro litigio, la empresa no se defenderá alegando que "tenía un manual de ética", sino demostrando que implementó controles técnicos verificables y auditable.

Aquí es donde el *legal design* se revela como la herramienta definitiva. Su valor no es estético, sino funcional: permite traducir las abstracciones de los reglamentos en una arquitectura organizativa operativa. Gracias a esta metodología, las obligaciones legales dejan de ser obstáculos para el equipo de IT y se convierten en especificaciones de diseño. El *legal design* es el puente que permite que el abogado y el ingeniero hablen el mismo idioma, transformando conceptos como la "explicabilidad" en interfaces que un supervisor humano pueda entender y gestionar realmente.

Por todo ello, la abogacía especializada debe dar un paso al frente y asumir un rol de diseño institucional. El jurista del siglo XXI no es un mero auditor que llega al final del proceso para dar el visto bueno; debe ser un arquitecto que participa desde la concepción del sistema. Esta metamorfosis exige perfiles híbridos que, sin necesidad de programar,

comprendan la lógica de la máquina para poder interrogarla y asegurar que respeta los derechos fundamentales y el propósito ético de la organización.

En conclusión, la gobernanza de la inteligencia artificial no es una cuestión tecnológica, sino esencialmente jurídica. La tecnología proporciona la potencia, pero es el derecho el que proporciona la dirección y el límite. Su éxito no dependerá de la complejidad de los algoritmos, sino de nuestra capacidad para integrar las garantías legales en la propia estructura de las organizaciones. El futuro de la justicia algorítmica se juega hoy en las mesas de diseño, donde el derecho debe dejar de ser un límite externo para convertirse en el motor de una innovación segura, ética y, sobre todo, responsable.