Vol. 7 – Núm. 1 / Enero - Junio – 2026

La redefinición del deber de diligencia del administrador societario en la era del big data: un análisis doctrinal y comparado desde la perspectiva ecuatoriana

The redefinition of the corporate director's duty of care in the big data era: a doctrinal and comparative analysis from the ecuadorian perspective

A redefinição do dever de diligência do administrador societário na era do big data: uma análise doutrinal e comparada sob a perspectiva equatoriana

Quiña Olmedo Emilly Alexandra[1]
Universidad Tecnológica Indoamérica
equina2@indoamerica.edu.ec
https://orcid.org/0009-0004-5746-3775

Molina Torres Maria Victoria[2]
Universidad Tecnológica Indoamérica
mariamolina@uti.edu.ec
https://orcid.org/0000-0003-3785-7916

DOI / URL: https://doi.org/10.55813/gaea/ccri/v7/n1/1558

Como citar:
Quiña Olmedo, E. A. & Molina Torres, M. V. (2026). La redefinición del deber de diligencia del administrador societario en la era del big data: un análisis doctrinal y comparado desde la perspectiva ecuatoriana. Código Científico Revista de Investigación, 7(1), 2421-2773.

***Recibido**: 15/04/2026* ***Aceptado**: 12/05/2026* ***Publicado**: 30/06/2026*

Resumen

El deber de diligencia del administrador societario atraviesa una transformación sustantiva por la incorporación de herramientas de *Big Data*, analítica predictiva e inteligencia artificial en la gestión empresarial. La investigación analiza, desde el derecho ecuatoriano y el derecho comparado, si la disponibilidad razonable de tecnologías capaces de procesar grandes volúmenes de datos modifica el contenido del deber de informarse previsto en el artículo 262 de la Ley de Compañías y, con ello, los límites de protección de la *business judgment rule*. El estudio adopta un diseño cualitativo de metodología jurídico-dogmática, hermenéutica, sistemática y comparada funcional. El corpus de análisis se integró por la Ley de Compañías, la Ley Orgánica de Protección de Datos Personales, la jurisprudencia de Delaware sobre deber de supervisión, el Reglamento (UE) 2024/1689, el marco NIST AI RMF 1.0 y los Principios de Gobierno Corporativo de la OCDE y del G20. La triangulación entre normas, doctrina especializada, jurisprudencia y documentos de *soft law* permitió construir criterios jurídicos aplicables a entornos decisorios informacionalmente complejos. Los resultados evidencian que el artículo 262 conserva una estructura abierta y flexible, pero insuficiente para orientar, por sí solo, la evaluación judicial de decisiones empresariales mediadas por sistemas algorítmicos. La omisión injustificada de herramientas predictivas accesibles, especialmente en sectores de alto riesgo o de intensa generación de datos, no debe tratarse como simple ejercicio de discrecionalidad estratégica, sino como un defecto del proceso decisorio. Como aporte central, se propone la figura del administrador como curador de datos y la adopción de un Expediente de Trazabilidad Algorítmica, escalable a las PYMES, que documente la selección de herramientas, la calidad de los datos, la auditoría de sesgos, la supervisión humana y la explicación razonable de los resultados utilizados. El estándar propuesto se modula por proporcionalidad, atendiendo a la dimensión de la empresa, el costo de implementación, la materialidad del riesgo y la brecha digital ecuatoriana.

Palabras clave: deber de diligencia; administrador societario; Big Data; business judgment rule; gobernanza algorítmica; responsabilidad fiduciaria.

Abstract

The corporate director’s duty of care is undergoing a substantive transformation as companies increasingly rely on Big Data, predictive analytics and artificial intelligence in business decision-making. This article examines, from an Ecuadorian and comparative law perspective, whether the reasonable availability of technologies capable of processing large datasets reshapes the duty to be informed under Article 262 of the Ecuadorian Companies Act and, consequently, the protective scope of the business judgment rule. The research follows a qualitative legal methodology based on doctrinal, hermeneutic, systematic and functional-comparative analysis. The analytical corpus includes the Ecuadorian Companies Act, the Ecuadorian Personal Data Protection Act, Delaware case law on directors’ oversight duties, Regulation (EU) 2024/1689, the NIST AI RMF 1.0 and the G20/OECD Principles of Corporate Governance. Triangulating statutory law, legal scholarship, case law and soft-law standards allowed the study to develop legal criteria for decision-making environments marked by informational complexity. The findings show that Article 262 remains open and adaptable, yet insufficient on its own to guide judicial assessment of business decisions mediated by algorithmic systems. The unjustified omission of accessible predictive tools, particularly in high-risk or data-intensive sectors, should not be treated merely as strategic discretion, but as a procedural defect in the decision-making process. The article proposes the concept of the

director as a data curator and the adoption of an Algorithmic Traceability Record, scalable for SMEs, documenting tool selection, data quality, bias auditing, human oversight and the reasoned explanation of algorithmic outputs. The proposed standard is adjusted through proportionality, taking into account company size, implementation costs, risk materiality and Ecuador's digital divide.

Keywords: duty of care; corporate director; Big Data; business judgment rule; algorithmic governance; fiduciary responsibility.

Resumo

O dever de diligência do administrador societário passa por uma transformação substantiva em razão da incorporação de ferramentas de Big Data, análise preditiva e inteligência artificial na gestão empresarial. A pesquisa examina, a partir do direito equatoriano e do direito comparado, se a disponibilidade razoável de tecnologias capazes de processar grandes volumes de dados altera o conteúdo do dever de informação previsto no artigo 262 da Lei de Companhias do Equador e, consequentemente, os limites de proteção da business judgment rule. O estudo adota um desenho qualitativo de metodologia jurídico-dogmática, hermenêutica, sistemática e comparada funcional. O corpus de análise foi integrado pela Lei de Companhias, pela Lei Orgânica de Proteção de Dados Pessoais, pela jurisprudência de Delaware sobre dever de supervisão, pelo Regulamento (UE) 2024/1689, pelo marco NIST AI RMF 1.0 e pelos Princípios de Governo Corporativo da OCDE e do G20. A triangulação entre normas, doutrina especializada, jurisprudência e documentos de soft law permitiu construir critérios jurídicos aplicáveis a ambientes decisórios informacionalmente complexos. Os resultados demonstram que o artigo 262 mantém uma estrutura aberta e flexível, mas insuficiente, por si só, para orientar a avaliação judicial de decisões empresariais mediadas por sistemas algorítmicos. A omissão injustificada de ferramentas preditivas acessíveis, especialmente em setores de alto risco ou de intensa geração de dados, não deve ser tratada como simples exercício de discricionariedade estratégica, mas como defeito procedimental do processo decisório. Como contribuição central, propõe-se a figura do administrador como curador de dados e a adoção de um Expediente de Rastreabilidade Algorítmica, escalável às PMEs, que documente a seleção de ferramentas, a qualidade dos dados, a auditoria de vieses, a supervisão humana e a explicação razoável dos resultados utilizados. O padrão proposto é modulado pela proporcionalidade, considerando a dimensão da empresa, o custo de implementação, a materialidade do risco e a brecha digital equatoriana.

Palavras-chave: dever de diligência; administrador societário; Big Data; business judgment rule; governança algorítmica; responsabilidade fiduciária.

Introducción

El deber de diligencia del administrador societario cumple una función estructural dentro del derecho de sociedades: fija el umbral mínimo de racionalidad exigible a quien gestiona intereses ajenos, administra riesgos empresariales y adopta decisiones con impacto patrimonial sobre socios, acreedores, trabajadores, consumidores y terceros. Su valor dogmático radica en que no opera como una lista cerrada de conductas, sino como un estándar

jurídico abierto, capaz de adaptarse a la complejidad económica de cada época. Esa apertura permitió que el tránsito desde el *bonus pater familias* hacia el ordenado empresario incorporara progresivamente criterios de profesionalidad, información suficiente, prudencia organizacional y control de riesgos.

La digitalización de la empresa introduce una dificultad de mayor densidad que las transformaciones organizativas anteriores. Las decisiones corporativas ya no descansan únicamente en estados financieros, informes gerenciales o experiencia sectorial acumulada. En mercados intensivos en datos, los administradores pueden acceder a herramientas capaces de detectar patrones, anticipar escenarios adversos, identificar anomalías, proyectar comportamientos de clientes, modelar incumplimientos contractuales y estimar riesgos operativos o reputacionales. La incertidumbre empresarial no desaparece, pero deja de ser un dato inevitable cuando existen medios técnicos razonables para reducirla.

La pregunta jurídica se vuelve entonces más exigente: si el administrador cuenta con herramientas predictivas accesibles, pertinentes y proporcionadas al riesgo de la decisión, ¿puede omitirlas sin afectar el deber de diligencia? La cuestión no admite una respuesta automática. El derecho societario debe evitar dos extremos: convertir la tecnología en una carga universal imposible de cumplir para toda compañía, o mantener una lectura analógica del deber de informarse que ignore la realidad de la gestión empresarial contemporánea. Entre ambos polos se ubica el problema central de esta investigación.

La tensión se concentra en la relación entre el deber de diligencia y la *business judgment rule*. Esta regla protege la discrecionalidad empresarial porque el juez no debe sustituir al administrador en la valoración del mérito económico de una decisión adoptada de buena fe, sin conflicto de interés y con información suficiente. Sin embargo, esa protección se justifica solo cuando la decisión proviene de un procedimiento razonable. En otras palabras, la regla no blinda el resultado; protege el proceso. Por ello, en entornos de *Big Data*, el análisis no debe limitarse

a preguntar si el negocio fracasó o si la decisión fue rentable, sino si el administrador desplegó un esfuerzo informativo proporcionado a la complejidad del riesgo.

El derecho comparado ofrece señales relevantes. En Delaware, la línea jurisprudencial que parte de *Caremark* y se consolida en decisiones como *Marchand v. Barnhill* e *In re Boeing Company Derivative Litigation* fortaleció el deber de supervisión del consejo frente a riesgos de misión crítica. Aunque esa tradición responde a un sistema jurídico distinto, su valor para el análisis ecuatoriano reside en la importancia que concede a los sistemas de información, monitoreo y reporte a nivel de administración. Si el deber de supervisión exige canales efectivos para riesgos materiales, resulta coherente examinar si, en empresas altamente dependientes de datos, esos canales deben incorporar herramientas de analítica predictiva, siempre que sean razonablemente accesibles.

En Ecuador, el artículo 262 de la Ley de Compañías, reformado en el marco de la modernización societaria, reconoce el estándar del ordenado empresario y articula la regla de la discrecionalidad empresarial en torno a cuatro presupuestos: buena fe, ausencia de interés personal, información suficiente y procedimiento decisorio adecuado. El avance normativo es significativo, pues desplaza la responsabilidad desde un juicio puramente retrospectivo sobre el resultado hacia una evaluación del proceso. La dificultad aparece cuando la norma debe aplicarse a decisiones mediadas por modelos algorítmicos, sistemas de recomendación, análisis predictivo o plataformas de riesgo cuya operación no siempre es transparente para el administrador ni para el juez.

La Ley Orgánica de Protección de Datos Personales añade otra dimensión al problema. El uso de datos para fines predictivos no puede entenderse solo como una práctica de eficiencia empresarial; también involucra principios de licitud, lealtad, transparencia, minimización, finalidad, privacidad desde el diseño y evaluación de impacto cuando el tratamiento entraña alto riesgo. Por ello, la información suficiente exigida al administrador no se agota en obtener

más datos. Debe tratarse de información jurídicamente obtenida, técnicamente confiable y sometida a controles que reduzcan sesgos, errores y afectaciones a derechos fundamentales.

El vacío que aborda este trabajo se ubica en la falta de un marco interpretativo ecuatoriano que permita determinar cuándo la disponibilidad razonable de herramientas de *Big Data* y analítica predictiva eleva el umbral de diligencia del administrador societario. La doctrina nacional ha desarrollado con mayor amplitud los deberes fiduciarios clásicos, la regla de discrecionalidad y el gobierno corporativo, pero aún no existe una construcción sistemática que conecte esos conceptos con gobernanza algorítmica, trazabilidad informacional y responsabilidad por confianza acrítica en resultados automatizados.

El objetivo general de la investigación es analizar críticamente la redefinición del deber de diligencia del administrador societario a partir de la incorporación de tecnologías de *Big Data* y análisis predictivo, con especial atención al artículo 262 de la Ley de Compañías ecuatoriana y al diálogo con estándares comparados. Como objetivos específicos se plantean: reconstruir dogmáticamente la evolución del estándar de diligencia; identificar los límites de la *business judgment rule* frente a decisiones algorítmicamente asistidas; examinar la interacción entre derecho societario y protección de datos personales; y proponer criterios operativos de trazabilidad que permitan distinguir entre discrecionalidad legítima y negligencia procedimental.

La hipótesis de trabajo sostiene que el artículo 262 puede interpretar el deber de diligencia en clave tecnológica, pero requiere criterios complementarios para hacerlo de manera jurídicamente segura. La omisión de herramientas predictivas no genera responsabilidad por sí misma. La responsabilidad surge cuando concurren, de forma acumulativa o altamente convergente, cuatro elementos: materialidad del riesgo, disponibilidad razonable de la herramienta, proporcionalidad económica de su implementación y ausencia de justificación documentada para prescindir de ella.

La relevancia del estudio es práctica y dogmática. Para los administradores, ofrece una guía de conducta basada en la documentación del proceso decisorio. Para los jueces, proporciona criterios de evaluación que evitan tanto la responsabilidad objetiva como la inmunidad injustificada. Para el legislador, identifica posibles líneas de mejora normativa. En una economía donde los datos son un insumo central de la gestión, el derecho societario no puede mantenerse ajeno a la pregunta por la calidad, trazabilidad y gobernanza de la información que sustenta las decisiones empresariales.

Metodología

La investigación se desarrolló bajo un diseño cualitativo de naturaleza jurídico-dogmática, con apoyo en la hermenéutica jurídica, el método sistemático y el derecho comparado funcional. Esta elección responde al objeto del estudio: no se busca medir empíricamente el grado de adopción de tecnologías predictivas por las empresas ecuatorianas, sino construir un marco interpretativo para evaluar el deber de diligencia del administrador cuando la decisión empresarial se apoya, o razonablemente pudo apoyarse, en información producida por sistemas de datos.

El enfoque dogmático permitió ordenar conceptos, identificar categorías normativas, precisar relaciones entre deberes fiduciarios y proponer criterios de imputación. En la investigación jurídica contemporánea, la dogmática no se reduce a describir normas vigentes; cumple una función reconstructiva cuando sistematiza principios, resuelve tensiones internas y formula soluciones coherentes con la estructura del ordenamiento (Van Hoecke, 2011). Desde esa perspectiva, el artículo 262 de la Ley de Compañías fue analizado como una cláusula abierta que requiere concreción a partir de la finalidad del deber de diligencia y del contexto tecnológico en que opera la administración societaria.

El método hermenéutico se empleó para interpretar las expresiones “diligencia de un ordenado empresario”, “información suficiente” y “procedimiento de decisión adecuado”. La

interpretación no se limitó al tenor literal de la norma; se consideraron su finalidad, su relación con el régimen de responsabilidad de administradores y su compatibilidad con estándares de gobierno corporativo. El método sistemático permitió conectar la Ley de Compañías con la Ley Orgánica de Protección de Datos Personales, especialmente en lo relativo a tratamiento lícito de datos, minimización, privacidad desde el diseño y evaluación de impacto.

El derecho comparado se utilizó con una orientación funcional, no trasplantista. La comparación no tuvo por objeto importar soluciones de Delaware o de la Unión Europea al derecho ecuatoriano, sino identificar problemas equivalentes y respuestas jurídicas útiles para construir criterios de evaluación. La literatura metodológica comparada advierte que la comparación jurídica exige atender a la función que cumple cada institución en su propio sistema y a los límites derivados del contexto normativo, económico e institucional de recepción (Siems, 2022). Por ello, la jurisprudencia de Delaware se examinó como referencia sobre deber de información y supervisión, mientras que el Reglamento (UE) 2024/1689 y el NIST AI RMF 1.0 se analizaron como marcos funcionales para graduar riesgos, documentar controles y exigir supervisión humana.

El corpus documental fue seleccionado mediante criterios de pertinencia jurídica, jerarquía normativa y calidad académica. Se incluyeron: (a) normas ecuatorianas aplicables al deber de diligencia y al tratamiento de datos personales; (b) jurisprudencia relevante de Delaware sobre *business judgment rule*, deber de información y deber de supervisión; (c) documentos institucionales de alto nivel sobre gobierno corporativo y gestión de riesgos de inteligencia artificial; y (d) doctrina académica especializada en derecho societario, derecho comparado, responsabilidad fiduciaria, gobernanza algorítmica y metodología jurídica. Se excluyeron fuentes enciclopédicas, entradas no académicas y materiales sin autoría verificable o sin relevancia directa para el objeto de estudio.

La técnica principal fue el análisis documental crítico. En primer lugar, se identificaron las categorías normativas del artículo 262 y se las vinculó con los presupuestos de la regla de discrecionalidad empresarial. En segundo lugar, se contrastó esa estructura con la doctrina del deber de informarse y con la evolución de la supervisión de riesgos de misión crítica. En tercer lugar, se examinó la interacción entre analítica predictiva y protección de datos personales. Finalmente, se formuló una matriz de criterios para determinar cuándo la omisión o el uso acrítico de herramientas algorítmicas puede configurar una infracción del deber de diligencia.

La validez interna del análisis se aseguró mediante triangulación normativa, doctrinal y jurisprudencial. La triangulación permitió evitar que la propuesta dependiera de una sola fuente o de una analogía aislada. Asimismo, se aplicó un criterio de proporcionalidad para adaptar los hallazgos al tejido empresarial ecuatoriano, caracterizado por una presencia significativa de pequeñas y medianas empresas. La investigación reconoce, por tanto, que el estándar de diligencia tecnológica no puede formularse como una obligación uniforme de incorporar sistemas sofisticados, sino como un deber graduado de buscar, evaluar, supervisar y documentar información razonablemente disponible según el riesgo y la capacidad de la compañía.

La limitación metodológica principal deriva de su carácter dogmático y documental. El estudio no presenta entrevistas, encuestas ni mediciones sobre adopción real de analítica predictiva en sociedades ecuatorianas. Esa decisión no resta validez al aporte, pero delimita su alcance: las conclusiones ofrecen criterios interpretativos y propuestas normativas, no diagnósticos empíricos sobre implementación tecnológica. Futuras investigaciones podrán contrastar la operatividad del Expediente de Trazabilidad Algorítmica mediante estudios de caso en sectores financiero, asegurador, comercial y cooperativo.

Resultados

Los resultados se ordenan en cinco ejes que responden a la pregunta central de la investigación: si el artículo 262 de la Ley de Compañías ofrece parámetros suficientes para

evaluar la diligencia del administrador en entornos empresariales mediados por *Big Data*, analítica predictiva e inteligencia artificial.

1. Mutación del estándar de diligencia

El análisis histórico-dogmático confirma que el deber de diligencia no es una categoría inmóvil. El *bonus pater familias* representó un estándar civil de prudencia ordinaria, adecuado para relaciones patrimoniales de menor complejidad. El ordenado empresario, en cambio, incorporó un grado superior de profesionalidad, propio de quien administra una organización económica y debe adoptar decisiones bajo riesgo. La digitalización introduce un tercer momento: el administrador ya no solo debe actuar con prudencia y experiencia, sino con capacidad para gestionar información técnica relevante.

La mutación no convierte al administrador en científico de datos ni en programador. Lo transforma en un sujeto jurídicamente obligado a comprender, al menos en términos funcionales, qué información necesita, qué herramienta puede proveerla, cuáles son sus límites y cómo documentar su uso. La diligencia deja de medirse solo por la rectitud subjetiva de la intención o por la razonabilidad económica del resultado. Pasa a evaluarse por la calidad del proceso informativo que antecede a la decisión.

De esta reconstrucción emergen dos categorías relevantes. La primera es la *culpa in eligendo* tecnológica, vinculada con la selección negligente de proveedores, modelos, fuentes de datos o sistemas de análisis. La segunda es la *culpa in vigilando* algorítmica, referida a la falta de supervisión crítica sobre resultados automatizados. Ambas categorías permiten precisar que el problema jurídico no es el error de la máquina en abstracto, sino la conducta del administrador frente al diseño, selección, control y documentación del sistema utilizado.

2. Relectura de la información suficiente en clave tecnológica

El artículo 262 exige que el administrador actúe con información suficiente y con arreglo a un procedimiento de decisión adecuado. La investigación muestra que esa suficiencia

no puede definirse de manera estática. En una empresa con bajo volumen de datos y riesgos ordinarios, la información suficiente puede provenir de reportes contables, análisis de mercado, asesoría profesional y deliberación interna. En una empresa financiera, aseguradora, tecnológica, sanitaria, logística o de consumo masivo, la suficiencia puede requerir mecanismos más robustos de detección, modelación y monitoreo de riesgos.

El hallazgo central es que la información suficiente debe entenderse como un estándar contextual. No equivale a recopilar toda la información posible, porque ello sería ineficiente e incompatible con la discrecionalidad empresarial. Tampoco se agota en consultar documentos tradicionales cuando el riesgo es previsible mediante herramientas accesibles. El estándar exige una relación razonable entre riesgo, costo, disponibilidad técnica, confiabilidad del modelo y capacidad de la compañía.

La Ley Orgánica de Protección de Datos Personales impone un límite decisivo: el administrador no puede perseguir más información a cualquier precio. La información útil para el deber de diligencia debe ser lícita, pertinente, minimizada y trazable. En consecuencia, el estándar de suficiencia se vuelve híbrido. Debe ser técnicamente idóneo para reducir incertidumbre empresarial y jurídicamente depurado para evitar vulneraciones de derechos, tratamientos excesivos o decisiones discriminatorias basadas en datos de baja calidad.

3. Insuficiencia del artículo 262 frente a la opacidad algorítmica

El artículo 262 ofrece una base normativa valiosa, pero no proporciona criterios específicos para evaluar decisiones asistidas por sistemas algorítmicos. Su apertura permite adaptación, pero también genera incertidumbre judicial. La norma no indica cuándo una herramienta predictiva era razonablemente exigible, cómo valorar la opacidad de un modelo, qué nivel de explicabilidad debe exigir el administrador ni qué documentación resulta necesaria para acreditar que el procedimiento decisorio fue adecuado.

La comparación con la jurisprudencia de Delaware permite sostener que la protección de la *business judgment rule* se debilita cuando el defecto no está en el resultado empresarial, sino en la falta de información o supervisión. *Smith v. Van Gorkom* mostró la importancia del proceso informativo antes de una decisión relevante. *Caremark*, *Marchand* e *In re Boeing* reforzaron la idea de que los consejos deben contar con sistemas razonables de monitoreo cuando enfrentan riesgos críticos. Trasladado al entorno de datos, el administrador que no implementa mecanismos proporcionados de seguimiento frente a riesgos modelizables puede quedar fuera del perímetro protector de la discrecionalidad empresarial.

No toda omisión tecnológica constituye negligencia. La responsabilidad requiere demostrar que la herramienta era pertinente, accesible, proporcional y capaz de incidir razonablemente en la comprensión del riesgo. Sin embargo, cuando esos elementos concurren y el administrador no deja constancia de una razón técnica, económica o jurídica para prescindir de la herramienta, la omisión deja de ser neutral. Se convierte en un defecto procedimental que afecta la premisa básica de una decisión informada.

4. Patrones de imputación en decisiones data-driven

La investigación identifica dos patrones de imputación especialmente relevantes. El primero es la omisión informativa relevante. Se presenta cuando existía una señal, alerta, dato o escenario predictivo razonablemente disponible sobre un riesgo material y el administrador no lo consideró, o lo descartó sin motivación documentada. En este supuesto, el daño no se imputa por el mero fracaso del negocio, sino por la ruptura del procedimiento racional que debía preceder a la decisión.

El segundo patrón es la confianza acrítica en un resultado algorítmico. El administrador puede apoyarse en expertos, informes técnicos y sistemas de análisis, pero esa confianza debe ser razonable. Un algoritmo no equivale automáticamente a un experto. Su utilización solo fortalece el proceso decisorio si el modelo ha sido seleccionado con diligencia, si sus datos son

adecuados, si sus límites son conocidos y si existe supervisión humana efectiva. Cuando el administrador se limita a obedecer un resultado automatizado sin comprender su alcance funcional, la tecnología deja de ser apoyo informativo y se convierte en sustitución indebida del juicio fiduciario.

Estos patrones permiten evitar una responsabilidad objetiva por resultados adversos. La responsabilidad no se activa porque la predicción falló, porque el modelo no anticipó todos los escenarios o porque el negocio generó pérdidas. Se activa cuando el administrador no puede explicar de forma razonable cómo eligió la información, cómo valoró sus límites y por qué adoptó una decisión determinada frente a riesgos detectables.

5. Gobernanza algorítmica y trazabilidad del proceso decisorio

El cruce entre derecho societario, protección de datos y estándares de inteligencia artificial permite proponer una graduación del deber de supervisión según el nivel de riesgo de la herramienta utilizada. La Tabla 1 sistematiza esa graduación en términos funcionales, sin trasladar mecánicamente categorías regulatorias extranjeras al derecho ecuatoriano.

Tabla 1
Niveles de supervisión algorítmica según el riesgo de la herramienta

Nivel de riesgo	Tipos de sistemas (ejemplos)	Intensidad del deber de supervisión
Riesgo bajo	Filtros de correo, optimización de inventarios, tableros descriptivos	Supervisión mínima, orientada a verificar funcionalidad, seguridad básica y coherencia operativa.
Riesgo medio	Segmentación de clientes, publicidad dirigida, evaluación comercial automatizada	Supervisión humana reactiva, revisión de sesgos básicos, trazabilidad de criterios y validación periódica de resultados.
Riesgo alto	Crédito, contratación de personal, salud, seguridad física, prevención de fraude o lavado de activos	Vigilancia humana activa, explicabilidad suficiente, auditoría de datos, documentación reforzada y posibilidad real de veto humano antes de producir efectos jurídicos o patrimoniales relevantes.

Nota. Elaboración propia con base en el análisis funcional del Reglamento (UE) 2024/1689, el NIST AI RMF 1.0 y los Principios de Gobierno Corporativo de la OCDE y del G20.

La tabla permite observar que el deber de diligencia no exige el mismo nivel de control para toda herramienta. Un filtro de correo o un tablero descriptivo no compromete, en principio, derechos o decisiones societarias críticas. En cambio, un sistema utilizado para aprobar créditos, contratar personal, detectar fraude o definir perfiles de clientes puede producir efectos relevantes sobre la compañía y sobre terceros. En esos casos, la supervisión humana no debe ser simbólica; debe permitir comprender, cuestionar y, si corresponde, detener el resultado automatizado.

El resultado más importante de la investigación es la propuesta del administrador como curador de datos. Esta categoría no pretende sustituir las nociones clásicas de diligencia, lealtad o supervisión; las actualiza frente a un entorno donde la calidad de la decisión depende de la calidad del ecosistema informacional. El administrador como curador de datos cumple cuatro funciones: seleccionar fuentes y herramientas con diligencia; verificar la calidad, licitud y pertinencia de los datos; supervisar críticamente los resultados algorítmicos; y documentar de manera trazable el proceso de decisión.

Para operacionalizar esta propuesta se plantea el Expediente de Trazabilidad Algorítmica. No se concibe como una carga burocrática uniforme, sino como un instrumento flexible, proporcional y escalable. En grandes compañías o sectores regulados puede requerir informes técnicos, auditorías externas, actas de comité y evaluaciones periódicas. En PYMES puede consistir en una matriz simplificada que documente la necesidad de la herramienta, el proveedor elegido, los datos utilizados, los riesgos identificados, la revisión humana y la justificación final de la decisión.

El expediente cumple una doble función. Antes de la decisión, disciplina el proceso interno y obliga a preguntar si la información disponible es suficiente y lícita. Después de la decisión, permite reconstruir la racionalidad del procedimiento y distinguir entre un riesgo

empresarial legítimo y una negligencia informativa. Así, la trazabilidad fortalece tanto la gestión como la defensa del administrador frente a eventuales acciones de responsabilidad.

Discusión

Los hallazgos permiten sostener que la redefinición del deber de diligencia no depende de una reforma tecnológica de la empresa, sino de una transformación del modo en que el derecho evalúa la racionalidad del proceso decisorio. La doctrina clásica de la *business judgment rule* nació para impedir que el juez reemplace al administrador en decisiones empresariales complejas. Esa finalidad conserva plena validez. Sin embargo, la deferencia judicial pierde fundamento cuando el procedimiento previo revela una renuncia injustificada a información relevante, accesible y proporcionada.

Bainbridge (2004) explica la *business judgment rule* como una doctrina de abstención judicial: los tribunales deben evitar la revisión sustantiva del mérito empresarial cuando el administrador actuó dentro de un ámbito legítimo de discrecionalidad. Esta tesis resulta compatible con el derecho ecuatoriano, pero exige precisar la condición de entrada a la deferencia. La abstención judicial no protege una decisión tomada sobre una base informativa insuficiente. En ese punto, la doctrina de Gurrea-Martínez (2018) aporta un criterio útil para jurisdicciones no estadounidenses: la regla puede incorporarse de forma eficiente solo si no produce incentivos de irresponsabilidad ni funciona como cheque en blanco para la administración.

El artículo 262 ecuatoriano recoge esa lógica al exigir buena fe, ausencia de interés personal, información suficiente y procedimiento adecuado. La dificultad aparece porque la norma no define cómo evaluar la suficiencia informativa en entornos de *Big Data*. Esta omisión no invalida la norma, pero obliga a una interpretación evolutiva. El ordenado empresario de la era digital no es quien adopta toda tecnología disponible, sino quien sabe justificar qué

información necesitaba, qué alternativas razonables tenía, por qué seleccionó o descartó determinados instrumentos y cómo controló los riesgos derivados de su uso.

La jurisprudencia de Delaware refuerza esta lectura. *Smith v. Van Gorkom* muestra que el proceso informativo puede ser jurídicamente relevante aun cuando el administrador actúe sin mala fe. *Caremark* y su evolución posterior evidencian que la supervisión de riesgos críticos exige sistemas de información efectivos. *Marchand v. Barnhill* y *In re Boeing* no convierten a los directores en garantes absolutos de la seguridad empresarial, pero sí rechazan una supervisión meramente formal cuando la compañía enfrenta riesgos centrales para su actividad. Este razonamiento es trasladable, con prudencia, a compañías ecuatorianas cuyo modelo de negocio depende de datos y predicciones.

El aporte de los estándares recientes de inteligencia artificial radica en que ofrecen lenguaje técnico para concretar deberes jurídicos abiertos. El Reglamento (UE) 2024/1689 insiste en supervisión humana, gestión de riesgos, documentación técnica y transparencia para sistemas de alto riesgo. El NIST AI RMF 1.0 estructura la gestión de riesgos de IA en funciones de gobernanza, mapeo, medición y gestión. Aunque ninguno de estos instrumentos regula directamente la responsabilidad societaria ecuatoriana, ambos ayudan a precisar qué significa un procedimiento razonable cuando la decisión se apoya en sistemas algorítmicos.

La interacción con la Ley Orgánica de Protección de Datos Personales impide una lectura puramente eficientista. La diligencia tecnológica no consiste en maximizar la captura de datos, sino en gobernar datos de manera lícita, necesaria y proporcional. Un administrador que utiliza información personal sin base jurídica, sin transparencia o sin evaluación de impacto cuando corresponde, no mejora su posición de diligencia; la compromete. La información suficiente debe ser también información legalmente utilizable.

En este punto se advierte una convergencia entre derecho societario y derecho de protección de datos. La privacidad desde el diseño, la evaluación de impacto y la minimización

no son obligaciones externas a la administración societaria. Integradas al deber de diligencia, se convierten en criterios de calidad del proceso decisorio. El administrador que ignora estas exigencias expone a la compañía a sanciones, litigios, pérdida reputacional y decisiones estratégicas fundadas en datos jurídicamente defectuosos.

La propuesta del administrador como curador de datos permite superar una visión limitada de la tecnología como simple herramienta de eficiencia. Curar datos supone seleccionar, depurar, contextualizar y supervisar información antes de convertirla en fundamento de una decisión fiduciaria. Esta categoría no impone al administrador competencias técnicas especializadas propias de un ingeniero, pero sí una alfabetización funcional suficiente para formular preguntas relevantes, exigir explicaciones razonables y no delegar acríticamente su juicio en proveedores o sistemas automatizados.

La confianza en expertos, tradicionalmente admitida en el gobierno corporativo, también requiere ajuste. Un experto humano puede explicar su metodología, asumir responsabilidad profesional y responder preguntas del órgano de administración. Un sistema algorítmico, en cambio, puede operar con opacidad, sesgos no detectados o datos de entrenamiento inadecuados. Por ello, la confianza en un algoritmo solo debe considerarse razonable si existe información mínima sobre su finalidad, límites, calidad de datos, desempeño esperado, riesgos conocidos y mecanismos de supervisión humana.

El Expediente de Trazabilidad Algorítmica cumple aquí una función probatoria y preventiva. Probatoria, porque permite acreditar que el administrador actuó con información suficiente y procedimiento adecuado. Preventiva, porque obliga a documentar ex ante los elementos que suelen reconstruirse tardíamente en un litigio: quién recomendó la herramienta, qué datos se usaron, qué riesgos se evaluaron, qué sesgos se revisaron, qué advertencias emitió el sistema y qué razones justificaron la decisión final. Su valor no reside en generar papeles, sino en preservar la racionalidad verificable del proceso.

La proporcionalidad es indispensable para evitar que el estándar se transforme en una carga irrealizable. Ecuador tiene un tejido empresarial heterogéneo, con grandes compañías capaces de implementar sistemas avanzados y PYMES que enfrentan limitaciones tecnológicas, financieras y humanas. El estándar propuesto no exige igualdad de medios, sino razonabilidad de esfuerzos. Una gran compañía financiera no puede alegar la misma capacidad informativa que una empresa familiar de baja complejidad. A la inversa, una PYME no queda liberada de todo deber tecnológico si maneja riesgos intensivos en datos y existen soluciones accesibles, graduales o sectoriales.

La consecuencia jurídica no debe formularse como negligencia automática por no usar inteligencia artificial. Esa posición sería excesiva y contraria a la lógica de la discrecionalidad empresarial. La tesis defendida es más precisa: cuando el riesgo es material, la herramienta es razonablemente accesible, su costo es proporcional, el sector la reconoce como práctica diligente y el administrador no documenta razones para omitirla, la protección de la *business judgment rule* se debilita. La negligencia no nace de no innovar, sino de decidir no saber cuando era razonable saber.

La discusión también tiene implicaciones judiciales. El juez societario no debe convertirse en auditor técnico del algoritmo ni evaluar retrospectivamente si el modelo elegido era el más sofisticado. Su tarea debe concentrarse en revisar el proceso: si se identificó el riesgo, si se buscó información pertinente, si se evaluaron alternativas, si se consultó asesoría adecuada, si se documentaron límites y si existió supervisión humana efectiva. Esta aproximación evita dos riesgos: una deferencia vacía frente a decisiones opacas y una responsabilidad objetiva encubierta por toda pérdida empresarial asociada a tecnología.

Desde una perspectiva de *lege ferenda*, el artículo 262 podría fortalecerse mediante una precisión normativa que incorpore la diligencia informacional en entornos tecnológicos. No sería conveniente incluir una lista cerrada de herramientas, porque la innovación volvería

obsoleta la norma en poco tiempo. Lo adecuado sería reconocer que, en sectores de alto riesgo o alta complejidad informacional, la suficiencia de la información puede requerir mecanismos proporcionales de analítica, trazabilidad, supervisión humana y documentación del proceso decisorio.

La investigación deja abierta una agenda empírica. Será necesario verificar cómo las compañías ecuatorianas adoptan herramientas predictivas, qué controles aplican, qué barreras enfrentan y cómo documentan sus decisiones. También conviene comparar la experiencia ecuatoriana con otros países latinoamericanos que han incorporado reglas de gobierno corporativo, protección de datos o transformación digital. Sin esa evidencia, la propuesta conserva valor dogmático, pero requiere validación práctica para convertirse en política legislativa o guía judicial consolidada.

Conclusiones

La investigación demuestra que el deber de diligencia del administrador societario se encuentra en una fase de redefinición profunda. La irrupción del *Big Data*, la analítica predictiva y la inteligencia artificial no elimina la discrecionalidad empresarial, pero cambia las condiciones bajo las cuales una decisión puede considerarse informada. El artículo 262 de la Ley de Compañías ofrece una base normativa adecuada al exigir información suficiente y procedimiento decisorio correcto, aunque resulta insuficiente para resolver por sí solo los problemas derivados de la opacidad algorítmica, la calidad de los datos y la supervisión humana de sistemas automatizados.

El principal aporte del estudio consiste en proponer la figura del administrador como curador de datos. Esta categoría permite comprender que la diligencia contemporánea no se agota en recibir informes o actuar de buena fe. Exige seleccionar herramientas y fuentes de información con prudencia, verificar la licitud y calidad de los datos, revisar sesgos, interpelar críticamente los resultados técnicos y documentar el razonamiento que conduce a la decisión.

La buena fe, sin un soporte informativo mínimo y verificable, pierde fuerza como argumento de exoneración cuando el riesgo era material y previsible mediante medios razonables.

La investigación también sostiene que la *business judgment rule* debe conservar su función protectora, pero solo cuando el administrador puede demostrar que actuó dentro de un procedimiento racional. La omisión de herramientas predictivas no genera responsabilidad automática. Sin embargo, cuando el riesgo era relevante, la tecnología estaba razonablemente disponible, el costo era proporcional y no existió justificación documentada para prescindir de ella, la omisión puede configurar negligencia procedimental y desplazar la protección de la regla de discrecionalidad.

El Expediente de Trazabilidad Algorítmica se propone como herramienta operativa para materializar el estándar. Su función es permitir la reconstrucción ex post del proceso decisorio mediante evidencia sobre selección de proveedores o modelos, calidad y licitud de datos, auditoría de sesgos, supervisión humana, explicabilidad y motivación de la decisión. Su diseño debe ser proporcional: reforzado para compañías grandes o sectores de alto riesgo, y simplificado para PYMES, sin perder su función esencial de documentar la racionalidad del proceso.

En el plano legislativo, el artículo 262 podría complementarse con criterios sobre diligencia informacional, gobernanza algorítmica y trazabilidad en sectores de alta complejidad. En el plano judicial, el análisis debe orientarse hacia la calidad del procedimiento y no hacia el éxito económico de la decisión. En el plano empresarial, la adopción de controles de datos no debe verse como formalidad, sino como una forma de proteger la gestión, reducir riesgos de agencia y fortalecer la defensa del administrador.

El límite estructural de la propuesta es la brecha digital ecuatoriana. Por esa razón, el estándar no puede formularse como una obligación uniforme de adoptar tecnologías avanzadas. Debe modularse según el tamaño de la compañía, el sector, la materialidad del riesgo, el costo

de implementación y la disponibilidad real de herramientas. La proporcionalidad permite que el deber de diligencia evolucione sin convertirse en una carga irrazonable.

La conclusión general es que el derecho societario ecuatoriano puede responder a la era del *Big Data* sin abandonar sus categorías fundamentales. Debe reinterpretarlas. El administrador diligente ya no es solo quien actúa honestamente y con prudencia empresarial; es quien gobierna la información que sustenta sus decisiones. En esa tarea, la trazabilidad algorítmica se convierte en el puente entre innovación tecnológica, responsabilidad fiduciaria y seguridad jurídica.

Referencias bibliográficas

Alfaro Águila-Real, J. (2020). La *business judgment rule*: mito y realidad. *Revista de Derecho de Sociedades*, 58, 101-130.

Aronson v. Lewis, 473 A.2d 805 (Del. 1984).

Bainbridge, S. M. (2004). The business judgment rule as abstention doctrine. *Vanderbilt Law Review, 57*(1), 83-130. https://scholarship.law.vanderbilt.edu/vlr/vol57/iss1/3/

Delaware General Corporation Law, 8 Del. C. § 141(e) (2023).

Enriques, L., & Zetzsche, D. A. (2020). Corporate technologies and the tech nirvana fallacy. *Hastings Law Journal, 72*(1), 55-98.

Floridi, L. (2021). *The ethics of artificial intelligence: Principles, challenges, and opportunities*. Oxford University Press.

Gurrea-Martínez, A. (2018). Re-examining the law and economics of the business judgment rule: Notes for its implementation in non-US jurisdictions. *Journal of Corporate Law Studies, 18*(2), 417-438. https://doi.org/10.1080/14735970.2017.1412688

In re Caremark International Inc. Derivative Litigation, 698 A.2d 959 (Del. Ch. 1996).

In re The Boeing Company Derivative Litigation, No. 2019-0907-MTZ, 2021 WL 4059934 (Del. Ch. Sept. 7, 2021).

Jensen, M. C., & Meckling, W. H. (1976). Theory of the firm: Managerial behavior, agency costs and ownership structure. *Journal of Financial Economics, 3*(4), 305-360. https://doi.org/10.1016/0304-405X(76)90026-X

King, K. M. (2021). *Marchand v. Barnhill*'s impact on the duty of oversight: New factors to assess directors' liability for breaching the duty of oversight. *Boston College Law Review, 62*(5), 1925-1964.

Knight, F. H. (1921). *Risk, uncertainty and profit*. Houghton Mifflin.

Ley de Compañías [Ecuador]. Registro Oficial No. 312, 5 de noviembre de 1999, reformada por el Tercer Suplemento del Registro Oficial No. 269, 15 de marzo de 2023.

Ley Orgánica de Protección de Datos Personales [Ecuador]. Registro Oficial Suplemento No. 459, 26 de mayo de 2021.

Marchand v. Barnhill, 212 A.3d 805 (Del. 2019).

Mayer-Schönberger, V., & Cukier, K. (2013). *Big data: A revolution that will transform how we live, work, and think*. Houghton Mifflin Harcourt.

National Institute of Standards and Technology. (2023). *Artificial intelligence risk management framework (AI RMF 1.0)* (NIST AI 100-1). U.S. Department of Commerce. https://doi.org/10.6028/NIST.AI.100-1

Organización para la Cooperación y el Desarrollo Económicos. (2024). *Principios de Gobierno Corporativo de la OCDE y del G20 2023*. OECD Publishing. https://doi.org/10.1787/fb38c737-es

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. *Diario Oficial de la Unión Europea*, L 2024/1689, 12 de julio de 2024.

Siems, M. (2022). *Comparative law* (3rd ed.). Cambridge University Press.

Smith v. Van Gorkom, 488 A.2d 858 (Del. 1985).

Van Hoecke, M. (Ed.). (2011). *Methodologies of legal research: Which kind of method for what kind of discipline?* Hart Publishing.

Yeung, K. (2019). *Responsibility and AI: A study of the implications of advanced digital technologies*. Council of Europe.

Zetzsche, D. A., Buckley, R. P., Arner, D. W., & Weber, R. H. (2020). The future of data-driven finance and RegTech: Lessons from EU Big Bang II. *Stanford Journal of Law, Business and Finance*, *25*(2), 245-288.