



Edition: Vol. 02 | N°. 01 | (2026)

Publication: 31/03/2026

DOI: <https://doi.org/10.70579/rfd.v2i1.152>

Inteligência regulatória digital: como IA e automação antecipam riscos legais e normativos em investigações de alta complexidade

Digital regulatory intelligence: how AI and automation anticipate legal and regulatory risks in highly complex investigations

Inteligencia regulatória digital: como IA y automatización anticipam riesgos legales y normativos en investigaciones de alta complejidad

Mario Vieira Quevedo

LEC – Legal, Ethics & Compliance

Especialista em Governança, Riscos e Compliance (GRC)

São Paulo, SP – Brasil

mariovieiraquevedo@gmail.com

RESUMO

A crescente complexidade dos ambientes regulatórios contemporâneos, especialmente no contexto das investigações internas corporativas mediadas por tecnologias digitais, tem desafiado os modelos tradicionais de fiscalização, investigação e controle jurídico. Nesse cenário, a incorporação da Inteligência Artificial e da automação às práticas regulatórias emerge como estratégia voltada à antecipação de riscos legais e normativos em investigações de alta complexidade. O presente trabalho tem por objetivo analisar criticamente o conceito de inteligência regulatória digital, compreendida como a articulação entre tecnologias algorítmicas, análise de dados e governança jurídica, examinando suas implicações para o monitoramento normativo e para a regulação da própria Inteligência Artificial. A pesquisa adota abordagem teórica e bibliográfica, com ênfase em autores do Direito Regulatório, da Governança, Riscos e *Compliance* (GRC), da governança algorítmica e da proteção de dados, buscando compreender de que modo a automação decisória reconfigura categorias jurídicas clássicas, como risco, responsabilidade, transparência e devido processo legal. Os resultados da análise indicam que a inteligência regulatória digital não se limita a uma inovação técnica, mas representa transformação estrutural da racionalidade regulatória, deslocando o foco do controle repressivo para modelos preventivos orientados por dados e análise preditiva. Conclui-se que a legitimação dessas práticas depende da construção de marcos normativos robustos, capazes de submeter o uso da Inteligência Artificial a princípios de transparência, proporcionalidade, supervisão humana significativa e responsabilização institucional,



Edition: Vol. 02 | Nº. 01 | (2026)

Publication: 31/03/2026

DOI: <https://doi.org/10.70579/rfd.v2i1.152>

assegurando compatibilidade entre eficiência regulatória, proteção de direitos e Estado de Direito.

Palavras-chave: governança algorítmica, inteligência artificial, inteligência regulatória digital, monitoramento normativo, risco jurídico.

ABSTRACT

The increasing complexity of two contemporary regulatory environments, especially in the context of internal corporate investigations mediated by digital technologies, has challenged the traditional models of oversight, investigation and legal control. In this context, the incorporation of Artificial Intelligence and automation into regulatory practices emerges as a strategy aimed at anticipating legal and regulatory risks in highly complex investigations. The present work aims to critically analyze the concept of digital regulatory intelligence, understood as the articulation between algorithmic technologies, data analysis and legal governance, examining its implications for regulatory monitoring and for the regulation of Artificial Intelligence itself. The research takes a theoretical and bibliographical approach, with emphasis on authors of Regulatory Law, Governance, Risks and Compliance (GRC), algorithmic governance and data protection, seeking to understand how automated decision-making reconfigures classic legal categories, such as risk, responsibility, transparency and debt legal process. The results of the analysis indicate that digital regulatory intelligence is not limited to technical innovation, but rather represents structural transformation of regulatory rationality, shifting the focus of repressive control to data-driven preventive models and predictive analysis. It is concluded that the legitimacy of these practices depends on the construction of robust regulatory frameworks, capable of subsuming the use of Artificial Intelligence to principles of transparency, proportionality, meaningful human supervision and institutional accountability, ensuring compatibility between regulatory efficiency, protection of rights and the State of Direito.

Keywords: algorithmic governance, artificial intelligence, digital regulatory intelligence, regulatory monitoring, legal risk.

RESUMEN

Una creciente complejidad de los ambientes regulatorios contemporáneos, especialmente en el contexto de las investigaciones internas corporativas mediadas por tecnologías digitales, tem desafiado os modelos tradicionales de fiscalización, investigación y control jurídico. En este escenario, la incorporación de la inteligencia artificial y la automatización de las prácticas reguladas emergen como estrategia voltada a la anticipación de riesgos legales y normativos en investigaciones de alta complejidad. El presente trabajo tiene como objetivo analizar críticamente el concepto de inteligencia regulatória digital, comprender como una articulación entre tecnologías algorítmicas,



Edition: Vol. 02 | N°. 01 | (2026)

Publication: 31/03/2026

DOI: <https://doi.org/10.70579/rfd.v2i1.152>

análisis de datos y gobernanza jurídica, examinando sus implicaciones para el monitoreo normativo y para una regulación de la propia inteligencia artificial. A pesquisa adota abordagem teórica y bibliográfica, com ênfase em autores do Direito Regulatório, da Governança, Riscos e Compliance (GRC), da gobernanza algorítmica e da proteção de dados, buscando compreender de que modo a automação decisória reconfigura categorias jurídicas clássicas, como risco, responsabilidade, transparencia y debido proceso legal. Los resultados del análisis indican que la inteligencia regulatória digital no se limita a una innovación técnica, pero representa una transformación estructural de la racionalidad regulatória, deslizando el foco del control represivo para modelos preventivos orientados por datos y análisis predictivo. Concluyendo que la legitimación de estas prácticas depende de la construcción de marcos normativos robustos, capaces de submeter o uso de inteligencia artificial a principios de transparencia, proporcionalidad, supervisión humana significativa y responsabilidad institucional, asegurando compatibilidad entre eficiencia regulatoria, protección de derechos y estado de derecho.

Palavras-chave: gobernanza algorítmica, inteligencia artificial, inteligencia regulatória digital, monitoramento normativo, riesgo jurídico.

1 INTRODUÇÃO

A intensificação da complexidade regulatória no contexto contemporâneo impõe desafios significativos ao Direito, especialmente diante da crescente digitalização das atividades econômicas, institucionais e administrativas. No âmbito das investigações internas corporativas, a multiplicação de normas, a fragmentação das fontes regulatórias e a atuação de agentes em ambientes transnacionais transformaram o risco jurídico de evento excepcional em elemento estrutural da governança regulatória, revelando a insuficiência dos modelos tradicionais de fiscalização e investigação diante de dinâmicas marcadas por alta velocidade decisória, opacidade informacional e circulação massiva de dados.

Essa insuficiência encontra raízes nos fundamentos clássicos do compliance corporativo, historicamente estruturado para lidar com riscos como corrupção, fraude, conflitos de interesse e violações éticas. Conforme destacam Coriolano e Cleórbete, “o compliance surge como mecanismo de identificação, análise e mitigação de riscos inerentes ao negócio, estruturando controles voltados à prevenção de sua concretização”.



Edition: Vol. 02 | Nº. 01 | (2026)

Publication: 31/03/2026

DOI: <https://doi.org/10.70579/rfd.v2i1.152>

Trata-se de uma racionalidade preventiva que, embora concebida para riscos analógicos, permanece essencial no ambiente digital.

Entretanto, o advento de tecnologias autônomas e sistemas de decisão algorítmica introduz riscos qualitativamente distintos, que desafiam essa arquitetura tradicional. A chamada Agentic AI, conforme observa Taimur Ijlal, “inaugura uma nova etapa da inteligência artificial, caracterizada pela autonomia operacional, pela execução de tarefas complexas sem supervisão contínua e pela capacidade de desencadear cadeias de ações imprevisíveis em infraestruturas corporativas”. Nesse contexto, os riscos deixam de ser exclusivamente humanos e passam a assumir natureza híbrida, combinando dimensões humanas, algorítmicas e sistêmicas.

Essa justaposição entre riscos tradicionais e emergentes evidencia que a inteligência regulatória digital não substitui o compliance clássico, mas o expande. A lógica preventiva permanece, porém, exige reconfiguração para operar em ambientes informacionais dinâmicos, marcados por decisões automatizadas e fluxos intensivos de dados. A incorporação da Inteligência Artificial e da automação às práticas regulatórias surge, assim, como resposta institucional à incapacidade humana de processar, em tempo adequado, grandes volumes de informações relevantes para o cumprimento normativo, especialmente em estruturas corporativas complexas.

No contexto brasileiro, o debate sobre regulação digital, proteção de dados e governança algorítmica ganhou centralidade com a consolidação de marcos normativos como a Lei Geral de Proteção de Dados Pessoais e o avanço de políticas públicas voltadas à digitalização da administração. Esses movimentos evidenciam a dupla posição da Inteligência Artificial no campo jurídico: simultaneamente como objeto de regulação e como instrumento utilizado pelo Estado e por organizações privadas para fins de fiscalização, controle e investigação interna.

Diante desse cenário, o problema que orienta este trabalho consiste em compreender de que modo a inteligência regulatória digital reconfigura o monitoramento normativo e a antecipação de riscos legais no âmbito das investigações internas



Edition: Vol. 02 | N°. 01 | (2026)

Publication: 31/03/2026

DOI: <https://doi.org/10.70579/rfd.v2i1.152>

corporativas de alta complexidade, bem como quais limites jurídicos devem ser observados para assegurar a compatibilidade dessas práticas com os princípios do Estado de Direito. Parte-se da hipótese de que a utilização da Inteligência Artificial no campo regulatório amplia a capacidade preventiva do Direito, ao mesmo tempo em que tensiona garantias fundamentais como o devido processo legal, a transparência decisória e a imputação de responsabilidade.

O objetivo geral da pesquisa é analisar criticamente os fundamentos jurídicos da inteligência regulatória digital, com foco na regulação da Inteligência Artificial e no uso de sistemas automatizados para monitoramento normativo em investigações internas corporativas. Como objetivos específicos, busca-se examinar a transformação da racionalidade regulatória diante da digitalização, analisar o papel da automação nas investigações de alta complexidade e identificar os limites jurídicos, institucionais e normativos da automação decisória no campo regulatório.

2 FUNDAMENTOS DO COMPLIANCE E GOVERNANÇA

A consolidação do compliance como disciplina estruturante da governança corporativa decorre de um movimento histórico voltado à resposta a riscos clássicos — corrupção, fraude, conflitos de interesse e violações éticas — por meio de mecanismos preventivos e controles internos. A literatura especializada destaca que o compliance surge como instrumento de racionalização organizacional, orientado à identificação, avaliação e mitigação de riscos capazes de comprometer a integridade institucional. Como afirmam Coriolano e Cleórbete, “*o compliance estrutura mecanismos capazes de prevenir a concretização de riscos inerentes ao negócio* (CORIOLANO; SANTOS, 2026).

Esse fundamento ético-preventivo permanece central, mesmo diante da crescente complexidade regulatória e tecnológica. O compliance não se limita a um conjunto de regras, mas configura um sistema de governança que articula cultura organizacional, controles internos, políticas corporativas e mecanismos de responsabilização. Segundo



Edition: Vol. 02 | Nº. 01 | (2026)

Publication: 31/03/2026

DOI: <https://doi.org/10.70579/rfd.v2i1.152>

DELFINO LAGROTA na obra *Compliance A–Z* (2026), ao sistematizar os principais conceitos da área, reforça que sua função é assegurar conformidade legal, integridade institucional e alinhamento entre conduta organizacional e expectativas regulatórias.

Compreender o compliance contemporâneo, contudo, exige ir além da dimensão normativa e incorporar a lógica sistêmica da governança corporativa. Nesse sentido, a abordagem de Governança, Riscos e Compliance (GRC) oferece arcabouço conceitual mais amplo. Essia e Ehiwario definem o GRC como “uma arquitetura integrada que permite às organizações atingir objetivos estratégicos, lidar com incertezas e agir com integridade, integração particularmente relevante em ambientes corporativos complexos, nos quais riscos jurídicos, operacionais, reputacionais e tecnológicos se entrelaçam.

A perspectiva do GRC desloca o compliance de uma função predominantemente reativa para um mecanismo de governança estratégica, capaz de antecipar riscos e orientar decisões. Em vez de atuar apenas sobre violações consumadas, o compliance passa a operar como sistema contínuo de monitoramento, análise e resposta, alinhado à cultura ética e à estratégia corporativa. Essa mudança assume especial relevância em ambientes digitais, marcados pela velocidade das operações e pela circulação massiva de dados.

Outro elemento essencial dos fundamentos do compliance é o papel da alta administração. Programas de integridade somente se tornam efetivos quando incorporados ao comportamento da liderança, responsável por estabelecer o chamado *tone at the top*. Sem esse compromisso institucional, políticas e controles tendem a se reduzir a formalidades, incapazes de influenciar práticas organizacionais. A governança contemporânea exige, portanto, atuação coordenada de conselhos, diretorias e comitês de risco, assegurando coerência entre discurso e prática.

Por fim, os fundamentos do compliance e do GRC convergem para uma mesma premissa: a integridade constitui ativo estratégico. Em mercados altamente regulados e expostos a riscos reputacionais, a capacidade de demonstrar conformidade, transparência e responsabilidade transforma-se em diferencial competitivo, preparando o terreno para a



Edition: Vol. 02 | Nº. 01 | (2026)
Publication: 31/03/2026
DOI: <https://doi.org/10.70579/rfd.v2i1.152>

articulação entre práticas anticorrupção, normas internacionais e sistemas de gestão na construção de ambientes corporativos íntegros e resilientes.

2.1 A COMPLEXIDADE REGULATÓRIA CONTEMPORÂNEA E A EROSÃO DOS MODELOS JURÍDICOS CLÁSSICOS

A digitalização das relações sociais, econômicas e institucionais promove profunda reconfiguração da racionalidade regulatória contemporânea, ao transformar os dados em elemento estruturante da tomada de decisão jurídica e administrativa. O avanço das tecnologias digitais possibilita a coleta, o armazenamento e o processamento contínuo de grandes volumes de informações, deslocando o eixo da regulação de modelos baseados em atos isolados para sistemas orientados pela análise permanente de padrões comportamentais e fluxos informacionais (Da Cruz, 2025).

Nesse contexto, o dado deixa de desempenhar função meramente acessória e passa a constituir fundamento central da ação regulatória. A capacidade de monitorar atividades em tempo real permite o desenvolvimento de estratégias mais sofisticadas de controle, baseadas na identificação antecipada de riscos e na mitigação preventiva de condutas potencialmente lesivas à ordem jurídica (Donato et al., 2022).

A incorporação dessa lógica informacional altera a função tradicional do Direito Regulatório, que passa a operar menos como instrumento repressivo e mais como mecanismo contínuo de gestão de riscos. A sanção perde centralidade, cedendo espaço a práticas de acompanhamento permanente, avaliação prospectiva e intervenção gradual, orientadas pela análise de dados e probabilidades (Saddy, 2020).

Todavia, a racionalidade regulatória orientada por dados não pode ser compreendida como avanço técnico neutro. Ela envolve escolhas normativas relevantes acerca das informações coletadas, dos padrões considerados relevantes e dos riscos priorizados, exigindo análise crítica quanto à sua compatibilidade com os princípios do Estado de Direito (Pereira, 2021).

A centralidade dos dados também reconfigura as relações de poder no campo regulatório, uma vez que o acesso, a capacidade de interpretação e o controle das



Edition: Vol. 02 | Nº. 01 | (2026)

Publication: 31/03/2026

DOI: <https://doi.org/10.70579/rfd.v2i1.152>

infraestruturas informacionais não se distribuem de forma equitativa entre os atores envolvidos. Essa assimetria pode comprometer a transparência das decisões regulatórias, especialmente quando estas se apoiam em modelos técnicos de difícil compreensão externa (Da Cruz, 2025).

Além disso, a dependência crescente de sistemas digitais complexos introduz riscos de opacidade decisória, dificultando o controle jurídico das decisões regulatórias e fragilizando o dever de motivação dos atos administrativos e investigativos (Pereira, 2021).

Nesse cenário, a exigência de transparência e explicabilidade dos sistemas digitais assume papel central na preservação da legitimidade do poder regulatório. A resposta a esses desafios não reside na rejeição da digitalização, mas na construção de marcos normativos capazes de submeter os sistemas baseados em dados aos mesmos princípios jurídicos que regem a atuação estatal tradicional, reconhecendo a tecnologia como instrumento subordinado ao Direito (Da Cruz, 2025).

Dessa forma, a reconfiguração da racionalidade regulatória promovida pela digitalização deve ser analisada simultaneamente como oportunidade e risco. A ampliação da capacidade de monitoramento e antecipação de condutas pode fortalecer a efetividade do Direito, desde que acompanhada de salvaguardas jurídicas robustas, aptas a preservar a transparência, a proporcionalidade e a responsabilização no exercício do poder regulatório (Donato et al., 2022).

2.2 INVESTIGAÇÕES DE ALTA COMPLEXIDADE E A EMERGÊNCIA DA INTELIGÊNCIA REGULATÓRIA DIGITAL

As investigações de alta complexidade assumem centralidade no debate contemporâneo sobre o uso de Inteligência Artificial e automação no Direito Regulatório, especialmente por se desenvolverem em ambientes marcados por elevada densidade normativa, fragmentação institucional e intensa circulação de dados. No campo da Governança, Riscos e Compliance (GRC) e do compliance investigativo, essa



Edition: Vol. 02 | N°. 01 | (2026)

Publication: 31/03/2026

DOI: <https://doi.org/10.70579/rfd.v2i1.152>

complexidade manifesta-se de forma particularmente intensa, uma vez que setores altamente regulados operam por meio de estruturas organizacionais transnacionais, cadeias decisórias distribuídas e tecnologias que desafiam os instrumentos tradicionais de investigação jurídica, ampliando os riscos de opacidade e de inefetividade regulatória (Aragão, 2020).

No ambiente corporativo, esse cenário envolve investigações internas caracterizadas por grandes volumes de documentos digitais, múltiplos stakeholders e interações distribuídas entre diferentes unidades organizacionais. Nessas situações, a insuficiência dos métodos investigativos clássicos torna-se evidente, uma vez que auditorias pontuais e análises retrospectivas não acompanham a velocidade, a complexidade e a sofisticação das operações reguladas, comprometendo a função preventiva do Direito (Coutinho, 2018).

A literatura jurídica nacional destaca que a dificuldade de reconstruir, de forma tempestiva, cadeias complexas de decisão e responsabilidade favorece a consolidação de riscos sistêmicos que escapam à fiscalização convencional. No contexto do compliance corporativo, essa limitação pode resultar em respostas tardias, aumento de sanções regulatórias e danos reputacionais relevantes, exigindo modelos investigativos mais integrados e prospectivos (Binenbojm, 2019).

A automação e o uso de sistemas baseados em Inteligência Artificial surgem, assim, como resposta funcional às limitações estruturais do modelo investigativo tradicional, ao possibilitar a análise integrada de grandes volumes de dados heterogêneos e a identificação de padrões comportamentais não perceptíveis por meios exclusivamente humanos. Essa transformação desloca a racionalidade da investigação regulatória e corporativa de uma lógica episódica para um modelo contínuo e prospectivo de monitoramento de riscos e inconformidades (Câmara, 2021).

Entretanto, a incorporação de decisões automatizadas em investigações de alta complexidade não se limita a uma questão de eficiência técnica, pois produz impactos jurídicos relevantes sobre categorias fundamentais como imputação de responsabilidade,



Edition: Vol. 02 | N°. 01 | (2026)

Publication: 31/03/2026

DOI: <https://doi.org/10.70579/rfd.v2i1.152>

motivação decisória e devido processo legal. A investigação passa a ser orientada por inferências probabilísticas e modelos preditivos, tensionando a tradição jurídica baseada na reconstrução causal de fatos e na individualização das condutas, especialmente em procedimentos internos suscetíveis de gerar sanções disciplinares ou comunicações a autoridades reguladoras (Ferraz Junior, 2021).

Ao operar por meio de correlações estatísticas, os sistemas automatizados tendem a deslocar o foco da infração consumada para o risco potencial. Essa antecipação pode ampliar a capacidade preventiva das organizações, mas também gerar intervenções baseadas em probabilidades que não correspondem, necessariamente, a comportamentos juridicamente censuráveis, exigindo critérios normativos rigorosos no âmbito dos programas de compliance (Aragão, 2020).

A opacidade dos sistemas de aprendizado de máquina agrava esses desafios, ao dificultar a reconstrução do raciocínio que conduz às decisões investigativas automatizadas. Quando os critérios utilizados pelo sistema não são compreensíveis ou auditáveis, enfraquece-se a possibilidade de contestação jurídica efetiva e compromete-se a exigência de motivação adequada das decisões investigativas internas (Binenbojm, 2019).

Além disso, a utilização de Inteligência Artificial em investigações complexas fragmenta a cadeia decisória entre múltiplos agentes humanos e sistemas técnicos, criando zonas de ambiguidade quanto à responsabilidade jurídica. Desenvolvedores, operadores, gestores de compliance e instâncias decisórias internas participam, em diferentes níveis, da produção dos resultados investigativos, o que desafia os modelos clássicos de imputação individual de responsabilidade (Ferraz Junior, 2021).

Do ponto de vista jurídico, é imprescindível afirmar que a responsabilidade pelas decisões automatizadas permanece humana e institucional, ainda que mediada por tecnologia. A delegação de funções investigativas à Inteligência Artificial não pode implicar transferência implícita de responsabilidade para sistemas técnicos, sob pena de



Edition: Vol. 02 | Nº. 01 | (2026)

Publication: 31/03/2026

DOI: <https://doi.org/10.70579/rfd.v2i1.152>

esvaziamento da accountability e fragilização da legitimidade dos programas de compliance e da atuação regulatória (Coutinho, 2018).

A governança jurídica das investigações automatizadas exige, portanto, marcos normativos e institucionais capazes de assegurar transparência, auditabilidade e proporcionalidade no uso da Inteligência Artificial. Esses marcos devem articular princípios do Direito Administrativo, do Direito Regulatório, do compliance corporativo e da proteção de dados pessoais, preservando a centralidade da responsabilidade jurídica e da proteção de direitos em ambientes investigativos cada vez mais mediados por sistemas inteligentes (Câmara, 2021).

2.3 CASOS CORPORATIVOS E RISCOS REGULATÓRIOS EM AMBIENTES DIGITAIS

A dinâmica das investigações internas corporativas pode ser ilustrada por casos reais que evidenciam como a complexidade regulatória, a fragmentação institucional e a circulação intensiva de dados moldam a atuação de órgãos reguladores e programas de compliance em ambientes digitais.

(a) Fraude contábil e governança corporativa — Caso Americanas (CVM):

Em 2023, a Comissão de Valores Mobiliários (CVM) instaurou processos administrativos para apurar indícios de fraude contábil envolvendo a Americanas S.A., relacionados a inconsistências bilionárias em operações de risco sacado. O caso evidenciou a necessidade de mecanismos contínuos de monitoramento de transações financeiras e de auditorias internas capazes de identificar padrões atípicos em tempo oportuno.¹

(b) Cartel e manipulação de mercado — Casos CADE

O Conselho Administrativo de Defesa Econômica (CADE) conduz investigações complexas sobre formação de cartel em setores como combustíveis, saúde e transporte

¹ Fonte oficial: <https://www.gov.br/cvm>



Edition: Vol. 02 | N°. 01 | (2026)

Publication: 31/03/2026

DOI: <https://doi.org/10.70579/rfd.v2i1.152>

público. Esses casos dependem, em grande medida, da análise massiva de comunicações internas, metadados e padrões de comportamento econômico, demonstrando a relevância de ferramentas automatizadas para a detecção de condutas coordenadas.²

(c) Assédio sistemático e governança trabalhista — Casos EEOC (EUA)

A Equal Employment Opportunity Commission (EEOC) tem conduzido investigações envolvendo assédio sistemático e discriminação estrutural, frequentemente baseadas na análise de grandes volumes de comunicações internas e registros de recursos humanos. Esses casos ilustram como a análise automatizada de dados pode auxiliar na identificação de padrões reiterados de conduta.³

Os casos apresentados demonstram que a complexidade investigativa não se limita ao plano teórico, manifestando-se em padrões operacionais recorrentes que podem ser sistematizados por meio de abordagens orientadas por dados.

2.4 NORMAS E SISTEMAS DE GESTÃO

A consolidação de programas de integridade e compliance depende, cada vez mais, da adoção de sistemas de gestão estruturados, capazes de integrar políticas, controles, processos e responsabilidades em uma arquitetura institucional coerente. Nesse contexto, normas internacionais como a ISO 37001 e a ISO 37301 desempenham papel central ao fornecer parâmetros objetivos para a implementação, operação e melhoria contínua de mecanismos de integridade corporativa.

A ISO 37001, dedicada a sistemas de gestão antissuborno, estabelece diretrizes para a prevenção, detecção e resposta a práticas corruptas, abrangendo políticas de integridade, controles financeiros, procedimentos de due diligence, investigações internas e monitoramento contínuo. O eBook Negro da ISO 37001 enfatiza que a norma não deve ser tratada como checklist burocrático, mas como arquitetura de integridade que exige transformação cultural e compromisso institucional (Echíchique, 2025). Essa perspectiva

² Fonte oficial: <https://www.gov.br/cade>

³ Fonte oficial: <https://www.eeoc.gov>



Edition: Vol. 02 | Nº. 01 | (2026)

Publication: 31/03/2026

DOI: <https://doi.org/10.70579/rfd.v2i1.152>

reforça que a certificação, isoladamente, não garante integridade, sendo a maturidade do sistema o fator determinante de sua efetividade.

De forma complementar, a ISO 37301, voltada a sistemas de gestão de compliance, amplia o escopo ao estabelecer requisitos para a implementação, manutenção e melhoria contínua de programas de conformidade. A Guia prática de compliance según la Norma ISO 37301 destaca que a norma consolida abordagem baseada em risco, governança e cultura organizacional, permitindo que as organizações adaptem seus programas às especificidades de seus setores e ambientes regulatórios (YsLa, 2021). A estruturação do compliance em torno do ciclo PDCA (Plan–Do–Check–Act) reforça a necessidade de planejamento estratégico, controles operacionais, monitoramento e melhoria contínua.

A integração entre as normas ISO 37001 e ISO 37301 fortalece a capacidade institucional de prevenir ilícitos, promover transparência e demonstrar diligência perante autoridades reguladoras. Essa integração articula-se com a abordagem de Governança, Riscos e Compliance (GRC), que compreende o compliance como parte de uma arquitetura mais ampla de governança corporativa. Essia e Ehiwario definem o GRC como um conjunto integrado de capacidades que permite às organizações atingir objetivos, lidar com incertezas e agir com integridade (Essia; Ehiwario, 2026), reforçando que sistemas de gestão não operam de forma isolada, mas como componentes de uma governança integrada.

A adoção de normas internacionais também contribui para a padronização de práticas investigativas, especialmente em ambientes digitais e de alta complexidade. A ISO 37301 exige o estabelecimento de procedimentos formais de investigação interna, com critérios de independência, documentação, rastreabilidade e imparcialidade, enquanto a ISO 37001 reforça a necessidade de due diligence contínua, sobretudo em cadeias de suprimentos e relações com terceiros, reduzindo riscos de corrupção transnacional.



Edition: Vol. 02 | Nº. 01 | (2026)

Publication: 31/03/2026

DOI: <https://doi.org/10.70579/rfd.v2i1.152>

Por fim, a maturidade dos sistemas de gestão depende da capacidade de integrar tecnologia, governança e cultura organizacional. Em ambientes regulatórios complexos, sistemas eficazes funcionam como infraestrutura institucional da inteligência regulatória digital, permitindo o monitoramento de riscos, a resposta a irregularidades e a demonstração de accountability perante autoridades reguladoras. Essa integração prepara o terreno para compreender como tecnologias emergentes, como a Inteligência Artificial, impactam a governança corporativa e os sistemas de gestão, tema desenvolvido na seção seguinte.

2.5 FRAUDE, CONTROLES E CONTABILIDADE FORENSE

A prevenção e a detecção de fraudes corporativas constituem elementos centrais da governança contemporânea, especialmente em ambientes regulatórios complexos e altamente digitalizados. A literatura especializada destaca que a fraude não é evento aleatório, mas fenômeno estruturado, resultante da interação entre incentivos, oportunidades e racionalizações individuais ou organizacionais. Sikander Sultan define fraude como “uma tentativa deliberada de obter vantagem indevida por meios ilícitos” (Sultan, 2021), ressaltando que sua natureza intencional a distingue de erros ou falhas operacionais.

No contexto corporativo, as fraudes assumem múltiplas formas, incluindo fraude ocupacional, manipulação de demonstrações financeiras, reconhecimento indevido de receitas, criação artificial de reservas (cookie jar reserves), práticas de big bath accounting e distorções contábeis destinadas a influenciar indicadores de desempenho. A contabilidade forense desempenha papel fundamental na identificação desses esquemas, ao combinar técnicas contábeis, auditoria investigativa e análise de dados para reconstruir eventos, identificar padrões atípicos e estabelecer nexos causais.

A literatura de fraud examination aprofunda essa distinção ao enfatizar que a fraude envolve manipulação intencional de fatos, situações ou percepções. Daniel



Edition: Vol. 02 | N°. 01 | (2026)

Publication: 31/03/2026

DOI: <https://doi.org/10.70579/rfd.v2i1.152>

Njuguna observa que “fraude é uma forma de engano deliberado, enraizada na manipulação intencional de informações” (Njuguna, 2025), reforçando a necessidade de metodologias estruturadas de investigação capazes de identificar sinais precoces, documentar evidências e sustentar decisões disciplinares ou regulatórias.

A compreensão dos fatores que impulsionam a fraude é frequentemente estruturada pelos modelos do Fraud Triangle e do Fraud Diamond, que destacam os elementos de pressão, oportunidade, racionalização e capacidade. Esses modelos auxiliam programas de compliance e auditoria na identificação de vulnerabilidades sistêmicas, especialmente em ambientes caracterizados por controles internos frágeis, processos opacos ou elevada assimetria informacional.

A contabilidade forense e os mecanismos de controle interno também desempenham papel essencial na prevenção de fraudes financeiras e operacionais. Controles como segregação de funções, trilhas de auditoria, reconciliações periódicas, monitoramento contínuo e due diligence de terceiros reduzem oportunidades de manipulação e fortalecem a governança corporativa. Em ambientes digitais, esses controles são potencializados por ferramentas de análise de dados e monitoramento automatizado, capazes de identificar anomalias em tempo real.

A investigação de fraudes corporativas exige abordagem multidisciplinar, integrando contabilidade, auditoria, tecnologia, governança e análise jurídica. Em investigações internas, a reconstrução de cadeias decisórias, a análise de metadados, a revisão de comunicações internas e a avaliação de transações financeiras são etapas essenciais para estabelecer responsabilidade e mitigar riscos regulatórios. A literatura especializada destaca que investigações eficazes dependem de independência, documentação adequada, rastreabilidade e fundamentação jurídica consistente.

Por fim, a análise de fraudes e controles internos conecta-se diretamente à inteligência regulatória digital. A capacidade de detectar padrões atípicos, antecipar riscos e reconstruir eventos complexos depende, cada vez mais, da integração entre contabilidade forense, auditoria digital e sistemas automatizados de monitoramento. Essa



Edition: Vol. 02 | N°. 01 | (2026)

Publication: 31/03/2026

DOI: <https://doi.org/10.70579/rfd.v2i1.152>

integração prepara o terreno para a discussão sobre tecnologias investigativas e inteligência aplicada, tema desenvolvido na seção seguinte.

2.6 TECNOLOGIA, INVESTIGAÇÃO E INTELIGÊNCIA

A crescente digitalização das atividades corporativas transformou profundamente a forma como investigações internas são conduzidas. A produção massiva de dados, a multiplicidade de dispositivos, a comunicação distribuída e a complexidade das infraestruturas tecnológicas exigem novas metodologias investigativas, capazes de integrar técnicas forenses, análise de dados e inteligência aplicada. Nesse contexto, a investigação corporativa deixa de ser processo exclusivamente jurídico ou contábil e passa a incorporar elementos típicos da investigação criminal tecnológica.

A prova digital tornou-se elemento central em investigações internas, especialmente em casos de fraude, assédio, manipulação de mercado, corrupção e incidentes cibernéticos. Jorge e Fausto destacam que a extração forense de dados exige rigor metodológico, preservação da cadeia de custódia e compreensão das limitações técnicas de cada método de coleta (Figueiredo; França Júnior, 2022). Técnicas como extração lógica, análise de backups, leitura de sistemas de arquivos e extração física permitem recuperar informações que abrangem comunicações, metadados, registros de localização e artefatos de aplicativos.

A investigação tecnológica também depende da capacidade de interpretar dados complexos e estabelecer vínculos entre pessoas, eventos e fluxos informacionais. Higor Jorge observa que, no âmbito da inteligência policial, “dado negado é todo conhecimento que não está disponível e cuja obtenção exige ação operacional” (Jorge, 2018). Essa lógica aplica-se diretamente ao ambiente corporativo, no qual a análise de vínculos, a reconstrução de cadeias decisórias e o mapeamento de redes de relacionamento são essenciais para compreender a dinâmica dos eventos investigados.

Ferramentas tecnológicas como softwares de análise de vínculos, plataformas de análise de dispositivos móveis, sistemas de mineração de dados e ferramentas de



Edition: Vol. 02 | Nº. 01 | (2026)

Publication: 31/03/2026

DOI: <https://doi.org/10.70579/rfd.v2i1.152>

monitoramento automatizado ampliam significativamente a capacidade investigativa. Essas tecnologias permitem identificar padrões comportamentais, detectar anomalias, correlacionar eventos e reconstruir fluxos de comunicação que seriam inviáveis de analisar manualmente.

A integração entre tecnologia e investigação exige, contudo, atenção à governança jurídica da prova digital. A coleta, o processamento e o armazenamento de dados devem observar princípios de proporcionalidade, finalidade, minimização e segurança, especialmente quando envolvem dados pessoais sensíveis. A ausência de critérios claros pode comprometer a validade da prova, gerar riscos regulatórios e fragilizar a legitimidade das conclusões investigativas.

Além disso, a investigação tecnológica amplia a necessidade de equipes multidisciplinares, capazes de articular conhecimentos jurídicos, contábeis, tecnológicos e operacionais. A atuação integrada de profissionais de compliance, auditoria, jurídico, tecnologia da informação e especialistas forenses permite análises mais robustas e reduz o risco de vieses interpretativos. A literatura especializada destaca que investigações eficazes dependem de independência, documentação adequada, rastreabilidade e fundamentação jurídica consistente.

Por fim, a convergência entre tecnologia, investigação e inteligência prepara o terreno para a discussão sobre sistemas autônomos e Inteligência Artificial aplicada ao contexto investigativo. A emergência da Agentic AI, com sua capacidade de perceber, raciocinar, agir e aprender de forma contínua, representa transformação estrutural na forma como organizações monitoram riscos e conduzem investigações internas, tema aprofundado na seção seguinte.

2.7 AGENTIC AI E O NOVO RISCO TECNOLÓGICO

A evolução recente da Inteligência Artificial inaugura um novo paradigma tecnológico que ultrapassa a lógica tradicional dos modelos generativos. A chamada Agentic AI representa mudança estrutural na forma como sistemas inteligentes percebem,



Edition: Vol. 02 | Nº. 01 | (2026)

Publication: 31/03/2026

DOI: <https://doi.org/10.70579/rfd.v2i1.152>

interpretam e interagem com o ambiente. Diferentemente da IA generativa clássica, baseada em respostas pontuais a comandos humanos, a Agentic AI opera por meio de ciclos contínuos de percepção, raciocínio, ação e aprendizado, ampliando significativamente sua autonomia operacional. Taimur Ijlal descreve esse fenômeno ao afirmar que “não se trata mais de uma IA de ‘perguntar e receber’, mas de uma IA que pensa, age e itera” (Ijlal, 2025).

Esse novo modelo de IA introduz riscos qualitativamente distintos daqueles tradicionalmente associados à automação. A capacidade de executar tarefas complexas sem supervisão contínua, interagir com múltiplos sistemas, acessar APIs, manipular dados sensíveis e desencadear cadeias de ações imprevisíveis amplia a superfície de ataque e cria novos vetores de risco. A literatura especializada identifica, entre esses riscos emergentes, práticas como prompt injection, memory poisoning, plugin hijacking, escalonamento não autorizado de privilégios e cascatas de erro decorrentes de decisões autônomas.

A autonomia operacional da Agentic AI desafia modelos tradicionais de governança e compliance. Em ambientes corporativos, sistemas autônomos podem interagir com bases de dados internas, executar rotinas automatizadas, tomar decisões pré-programadas e acionar fluxos operacionais sem intervenção humana direta. Isso exige mecanismos de controle capazes de monitorar ações autônomas, registrar trilhas de auditoria, limitar permissões e estabelecer salvaguardas para prevenir comportamentos inesperados ou indesejados.

Do ponto de vista regulatório, a Agentic AI tensiona categorias jurídicas clássicas como responsabilidade, causalidade e supervisão humana. A fragmentação da cadeia decisória entre agentes humanos e sistemas autônomos cria zonas de ambiguidade quanto à imputação de responsabilidade por danos ou violações normativas. A literatura especializada enfatiza que a supervisão humana significativa permanece elemento indispensável para assegurar accountability, proporcionalidade e compatibilidade com os princípios do Direito Administrativo e Regulatório.



Edition: Vol. 02 | Nº. 01 | (2026)

Publication: 31/03/2026

DOI: <https://doi.org/10.70579/rfd.v2i1.152>

A emergência da Agentic AI impacta diretamente as investigações internas corporativas. Sistemas autônomos podem gerar, modificar ou excluir dados, interagir com sistemas de comunicação, acionar fluxos operacionais e influenciar processos decisórios. Isso exige que programas de compliance e auditoria incorporem controles específicos para monitorar o comportamento desses sistemas, identificar desvios, registrar logs detalhados e garantir a integridade da prova digital. A ausência de mecanismos robustos de governança pode comprometer investigações, dificultar reconstruções fáticas e fragilizar a responsabilização institucional.

Além disso, a Agentic AI amplia a necessidade de integração entre governança tecnológica, gestão de riscos e compliance. Modelos tradicionais de GRC, baseados em controles estáticos e avaliações periódicas, tornam-se insuficientes diante de sistemas capazes de aprender, adaptar-se e modificar seu comportamento ao longo do tempo. A literatura especializada destaca a necessidade de abordagens dinâmicas de governança, com monitoramento contínuo, testes adversariais, validação de modelos e auditorias algorítmicas.

Por fim, a compreensão dos riscos associados à Agentic AI é fundamental para a consolidação da inteligência regulatória digital. A capacidade de antecipar riscos, monitorar comportamentos autônomos e estabelecer salvaguardas jurídicas adequadas será determinante para assegurar que a adoção de sistemas autônomos ocorra de forma ética, segura e compatível com o Estado de Direito, temas retomados na seção final.

2.8 INTELIGÊNCIA REGULATÓRIA DIGITAL: FUNDAMENTOS, APLICAÇÕES E LIMITES JURÍDICOS

A inteligência regulatória digital emerge no contexto de profundas transformações estruturais das práticas regulatórias contemporâneas, impulsionadas pela intensificação da complexidade normativa, pela digitalização das atividades econômicas e institucionais e pela centralidade dos dados na gestão pública e corporativa. Não se trata da mera adoção instrumental de tecnologias, mas de uma reconfiguração da racionalidade regulatória, na



Edition: Vol. 02 | N°. 01 | (2026)

Publication: 31/03/2026

DOI: <https://doi.org/10.70579/rfd.v2i1.152>

qual a análise automatizada de informações, a modelagem preditiva e o monitoramento contínuo passam a desempenhar papel central na identificação e mitigação de riscos jurídicos e normativos (Aragão, 2020).

Do ponto de vista conceitual, a inteligência regulatória digital pode ser compreendida como a integração entre Inteligência Artificial, automação e governança jurídica, orientada à construção de sistemas capazes de observar, interpretar e antecipar comportamentos relevantes para a aplicação do Direito Regulatório. Essa integração desloca o eixo da regulação de uma lógica predominantemente reativa, centrada na repressão ex post, para um modelo prospectivo, no qual a prevenção de danos e a gestão estratégica de riscos assumem primazia (Coutinho, 2018).

A consolidação desse modelo está diretamente relacionada à incapacidade dos mecanismos tradicionais de fiscalização e investigação de lidar com ambientes regulatórios caracterizados por múltiplos níveis normativos, operações transnacionais e fluxos informacionais intensivos. Em estruturas corporativas complexas, marcadas pela circulação massiva de dados digitais, a análise exclusivamente humana revela-se insuficiente para assegurar respostas tempestivas e eficazes aos riscos regulatórios emergentes, exigindo instrumentos tecnológicos capazes de operar em escala e velocidade compatíveis com a realidade investigativa contemporânea (Câmara, 2021).

Sob a perspectiva jurídica, a inteligência regulatória digital implica redefinição das categorias tradicionais do Direito Regulatório, especialmente no que se refere à natureza da decisão administrativa e investigativa. A decisão deixa de ser concebida como ato isolado fundado exclusivamente na subsunção normativa e passa a resultar de processos contínuos de avaliação, nos quais normas jurídicas dialogam permanentemente com indicadores empíricos, métricas de conformidade e sinais de risco produzidos por sistemas orientados por dados (Aragão, 2020).

Esse deslocamento impacta diretamente o papel das autoridades reguladoras e das instâncias internas de compliance, que passam a atuar como gestoras de ecossistemas normativos complexos, orientando sua atuação a partir de sinais de risco identificados por



Edition: Vol. 02 | Nº. 01 | (2026)

Publication: 31/03/2026

DOI: <https://doi.org/10.70579/rfd.v2i1.152>

sistemas automatizados. A inteligência regulatória digital permite priorizar apurações, calibrar respostas investigativas e estruturar fluxos decisórios mais eficientes, desde que preservada a centralidade da avaliação jurídica humana e da fundamentação normativa adequada (Câmara, 2021).

Entretanto, a eficiência técnica não pode se converter em critério exclusivo de legitimação da atuação regulatória automatizada. A definição dos dados analisados, dos padrões considerados relevantes e dos limiares de risco incorporados aos sistemas reflete escolhas normativas que devem ser submetidas a controle jurídico, institucional e ético, especialmente quando produzem efeitos relevantes sobre direitos individuais e coletivos (Binenbojm, 2019).

Dessa forma, a inteligência regulatória digital deve ser compreendida como prática normativa situada no interior de disputas jurídicas e institucionais sobre os limites do poder regulatório. Sua legitimação depende da construção de marcos jurídicos capazes de assegurar transparência, supervisão humana significativa e responsabilização institucional, preservando a centralidade do Direito na mediação entre inovação tecnológica, eficiência regulatória e proteção de direitos fundamentais (Câmara, 2021).

2.9 APLICAÇÕES PRÁTICAS E MONITORAMENTO NORMATIVO AUTOMATIZADO

A aplicação prática da inteligência regulatória digital em investigações internas decorre da crescente incapacidade dos modelos tradicionais de apuração de lidar com ambientes corporativos caracterizados por elevada complexidade normativa, massificação de dados digitais e estruturas organizacionais distribuídas. Em contextos nos quais comunicações eletrônicas, registros sistêmicos e documentos digitais constituem a principal base probatória, a atuação investigativa passa a depender de ferramentas capazes de organizar, filtrar e priorizar informações em escala compatível com a realidade organizacional contemporânea (Aragão, 2020).



Edition: Vol. 02 | Nº. 01 | (2026)

Publication: 31/03/2026

DOI: <https://doi.org/10.70579/rfd.v2i1.152>

No âmbito brasileiro, diretrizes institucionais voltadas à condução de processos administrativos e investigações internas reconhecem que procedimentos envolvendo grandes volumes de dados digitais não podem ser conduzidos exclusivamente por análise manual. A Controladoria-Geral da União destaca a utilização de instrumentos tecnológicos para triagem documental, indexação de informações e organização de evidências digitais, sempre sob supervisão humana e com finalidade investigativa delimitada (Controladoria-Geral da União, 2018).

Em investigações internas corporativas, essa aplicação se manifesta na análise de acervos massivos de e-mails corporativos, registros de sistemas financeiros, logs de acesso e bases documentais internas, cujo volume inviabiliza a leitura individualizada. Ferramentas baseadas em automação e análise de dados permitem a clusterização temática, a identificação de recorrência de termos sensíveis e a priorização de conjuntos informacionais relevantes, direcionando o esforço investigativo para núcleos de maior risco regulatório (Coutinho, 2018).

Experiências brasileiras em investigações concorrenciais e acordos de leniência também evidenciam o uso de instrumentos tecnológicos como suporte à organização e ao tratamento de grandes massas documentais. O Conselho Administrativo de Defesa Econômica reconhece que, em procedimentos complexos, a racionalização do tratamento de documentos digitais constitui condição para a efetividade da apuração, sem que isso implique substituição do juízo jurídico pela tecnologia (Cade, 2016).

Essas práticas demonstram que a inteligência regulatória digital atua como infraestrutura de apoio qualificado à tomada de decisão jurídica, e não como instância decisória autônoma. Os sistemas utilizados auxiliam na identificação de padrões, correlações e indícios relevantes, mas a interpretação jurídica, a valoração das provas e a definição das medidas investigativas permanecem sob responsabilidade humana e institucional, preservando a lógica do devido processo administrativo e investigativo (Binenbojm, 2019).



Edition: Vol. 02 | Nº. 01 | (2026)

Publication: 31/03/2026

DOI: <https://doi.org/10.70579/rfd.v2i1.152>

No contexto dos programas de integridade e compliance corporativo, a inteligência regulatória digital também se expressa por meio do monitoramento normativo automatizado, orientado à antecipação de riscos legais. A observação contínua de condutas reguladas, mediada por sistemas capazes de processar grandes volumes de dados em tempo real, permite identificar sinais precoces de inconformidade e estruturar respostas graduais e proporcionais, superando os limites da fiscalização episódica tradicional (Câmara, 2021).

Todavia, a antecipação de riscos por meio do monitoramento automatizado exige delimitação jurídica rigorosa. A ampliação da capacidade de vigilância interna pode gerar intervenções excessivamente invasivas, especialmente quando envolve dados pessoais e comunicações privadas de colaboradores. Por essa razão, a literatura jurídica enfatiza que tais práticas devem observar limites derivados da legislação de proteção de dados, da proporcionalidade e da finalidade investigativa legítima (Mendes, 2020).

Outro desafio relevante refere-se à opacidade dos critérios utilizados pelos sistemas tecnológicos, que pode dificultar a reconstrução do raciocínio investigativo e comprometer a motivação das decisões internas. A ausência de rastreabilidade adequada fragiliza tanto o direito de defesa dos investigados quanto a legitimidade institucional do procedimento, exigindo que os sistemas utilizados sejam auditáveis e passíveis de explicação em linguagem juridicamente compreensível (Ferraz Junior, 2021).

Além disso, a fragmentação da cadeia decisória constitui desafio central. Em investigações apoiadas por tecnologia, múltiplos atores — gestores, equipes de compliance, consultores externos e sistemas técnicos — participam da produção dos resultados investigativos. A governança da inteligência regulatória digital exige, portanto, definição clara de responsabilidades, evitando a diluição da accountability e assegurando que decisões investigativas possam ser juridicamente imputadas a instâncias humanas identificáveis (Binenbojm, 2019).

Dessa forma, as aplicações práticas e o monitoramento normativo automatizado evidenciam que a inteligência regulatória digital pode ampliar significativamente a



Edition: Vol. 02 | N°. 01 | (2026)

Publication: 31/03/2026

DOI: <https://doi.org/10.70579/rfd.v2i1.152>

capacidade preventiva e organizacional do Direito, desde que inserida em arranjos institucionais juridicamente estruturados. Sua legitimação depende da articulação entre eficiência investigativa, supervisão humana significativa, transparência procedimental e proteção de direitos fundamentais, preservando a centralidade do Direito na condução de investigações em ambientes corporativos complexos (Câmara, 2021).

2.10 LIMITES JURÍDICOS, VIESES E RESPONSABILIDADE INSTITUCIONAL

A incorporação de sistemas automatizados e de Inteligência Artificial à tomada de decisão no campo jurídico-regulatório impõe a necessidade de delimitar com precisão seus limites jurídicos, uma vez que tais tecnologias, ao influenciarem diretamente a produção de efeitos normativos relevantes, podem tensionar princípios estruturantes do Estado de Direito se não forem submetidas a critérios normativos claros e a mecanismos eficazes de controle institucional (Aragão, 2020).

Entre os principais desafios associados às decisões automatizadas destaca-se a problemática dos vieses estruturais incorporados aos sistemas tecnológicos, que podem emergir tanto dos dados utilizados quanto das escolhas normativas e metodológicas realizadas em seu desenho. Esses vieses, ainda que não intencionais, possuem potencial para reproduzir desigualdades preexistentes, produzindo impactos discriminatórios indiretos incompatíveis com o princípio da igualdade jurídica e com a função garantidora do Direito Administrativo (Binenbojm, 2019).

A identificação e a mitigação desses vieses mostram-se particularmente complexas em sistemas baseados em aprendizado de máquina, cuja lógica interna frequentemente não é plenamente acessível aos operadores jurídicos. A opacidade técnica dificulta a reconstrução dos critérios que conduziram à decisão automatizada, comprometendo a transparência administrativa e a possibilidade de controle jurídico e institucional das práticas regulatórias mediadas por tecnologia (Câmara, 2021).



Edition: Vol. 02 | N°. 01 | (2026)

Publication: 31/03/2026

DOI: <https://doi.org/10.70579/rfd.v2i1.152>

Essa dificuldade possui implicações diretas sobre o direito de defesa e o contraditório, na medida em que o destinatário da decisão encontra obstáculos para compreender os fundamentos que justificaram a intervenção regulatória ou investigativa. A ausência de explicabilidade adequada fragiliza a legitimidade jurídica das decisões e limita a efetividade do controle jurisdicional e administrativo, especialmente em procedimentos que produzem efeitos sancionatórios ou restritivos de direitos (Ferraz Junior, 2021).

Outro aspecto central refere-se à responsabilidade jurídica decorrente das decisões automatizadas. A mediação tecnológica tende a fragmentar a cadeia decisória entre diferentes agentes humanos, estruturas organizacionais e sistemas técnicos, dificultando a imputação clara de responsabilidade e criando zonas de ambiguidade normativa que enfraquecem a accountability institucional (Binenbojm, 2019).

Do ponto de vista jurídico, é fundamental afirmar que a utilização de sistemas automatizados não desloca a responsabilidade para a tecnologia em si. A responsabilidade permanece humana e institucional, exigindo a identificação clara dos agentes responsáveis pelo desenvolvimento, pela implementação e pela supervisão dos sistemas utilizados, sob pena de esvaziamento do princípio da imputabilidade no Direito Público e no compliance corporativo (Aragão, 2020).

Além disso, a automação decisória influencia a intensidade e a frequência das intervenções regulatórias, especialmente quando baseada em modelos preditivos orientados por probabilidades. A antecipação de riscos, se não for adequadamente limitada por critérios normativos e procedimentais, pode conduzir à adoção de medidas excessivamente restritivas, tensionando os princípios da proporcionalidade e da razoabilidade que orientam a atuação administrativa legítima (Câmara, 2021).

A dependência excessiva de sistemas automatizados pode ainda produzir a naturalização das decisões tecnológicas, conferindo-lhes aparência de neutralidade técnica que obscurece os juízos normativos incorporados ao seu funcionamento. Esse fenômeno reduz o espaço para deliberação jurídica crítica e enfraquece o papel do Direito



Edition: Vol. 02 | Nº. 01 | (2026)

Publication: 31/03/2026

DOI: <https://doi.org/10.70579/rfd.v2i1.152>

como instância de mediação entre eficiência regulatória, governança institucional e proteção de direitos fundamentais (Ferraz Junior, 2021).

Diante desse cenário, a governança jurídica da inteligência regulatória digital exige a construção de marcos normativos capazes de impor obrigações de transparência, auditabilidade e supervisão humana significativa sobre os sistemas utilizados na tomada de decisão regulatória e investigativa. Esses mecanismos reduzem riscos de arbitrariedade, fortalecem a accountability institucional e preservam a legitimidade do exercício do poder regulatório em ambientes tecnologicamente mediados (Aragão, 2020).

A análise dos limites jurídicos, dos vieses estruturais e da responsabilidade institucional evidencia, assim, que a incorporação da Inteligência Artificial ao campo regulatório exige governança jurídica rigorosa, capaz de assegurar que a busca por eficiência e antecipação de riscos não se sobreponha à preservação das garantias fundamentais e à centralidade do Estado de Direito (Ferraz Junior, 2021).

3 METODOLOGIA

A presente investigação desenvolve-se a partir de uma abordagem qualitativa, de natureza teórica e interpretativa, orientada pela análise crítica de produções acadêmicas e normativas relacionadas ao Direito Regulatório, à governança corporativa, à proteção de dados e à inteligência artificial aplicada ao contexto jurídico. A escolha dessa estratégia metodológica decorre da complexidade do objeto de estudo, que não se limita à descrição de fenômenos empíricos, mas exige a compreensão de transformações estruturais na racionalidade regulatória contemporânea.

O percurso metodológico fundamenta-se na pesquisa bibliográfica e documental, com levantamento sistemático de obras especializadas, artigos científicos, marcos normativos nacionais e internacionais, além de documentos institucionais vinculados à Governança, Riscos e Compliance (GRC) e à regulação tecnológica. Foram privilegiadas fontes que abordam a interface entre tecnologia, regulação e governança algorítmica,



Edition: Vol. 02 | N°. 01 | (2026)

Publication: 31/03/2026

DOI: <https://doi.org/10.70579/rfd.v2i1.152>

permitindo examinar de forma articulada os impactos da automação decisória sobre categorias jurídicas clássicas, como responsabilidade, transparência e devido processo legal .

Do ponto de vista analítico, adotou-se uma abordagem crítico-dedutiva, na qual conceitos consolidados do Direito são revisitados à luz das transformações promovidas pela digitalização e pela incorporação de sistemas inteligentes nos processos regulatórios. Esse movimento possibilita não apenas descrever o fenômeno da inteligência regulatória digital, mas também problematizar suas implicações jurídicas, institucionais e éticas, especialmente no contexto das investigações internas corporativas de alta complexidade.

A organização do material analisado ocorreu por meio de eixos temáticos estruturantes, que orientaram o desenvolvimento do estudo: (i) fundamentos do compliance e da governança; (ii) reconfiguração da racionalidade regulatória em ambientes digitais; (iii) investigações corporativas e complexidade normativa; (iv) integração entre tecnologia, inteligência e práticas investigativas; e (v) limites jurídicos da automação decisória. Essa sistematização permitiu identificar convergências teóricas, lacunas normativas e tensões entre eficiência regulatória e proteção de direitos fundamentais.

Adicionalmente, foram incorporadas análises de casos institucionais e práticas regulatórias contemporâneas, com o objetivo de aproximar a reflexão teórica de situações concretas enfrentadas por órgãos reguladores e programas de compliance. Embora não se trate de pesquisa empírica, a utilização desses exemplos contribui para ilustrar a aplicabilidade dos conceitos discutidos e reforçar a dimensão prática do fenômeno analisado.

A interpretação dos dados foi conduzida de forma reflexiva e crítica, buscando evidenciar como a incorporação da Inteligência Artificial e da automação não representa apenas uma inovação instrumental, mas uma mudança paradigmática na forma de atuação do Direito Regulatório. Nesse sentido, a metodologia adotada permite compreender a inteligência regulatória digital como fenômeno jurídico complexo, situado na interseção



Edition: Vol. 02 | N°. 01 | (2026)

Publication: 31/03/2026

DOI: <https://doi.org/10.70579/rfd.v2i1.152>

entre tecnologia, governança e proteção de direitos, contribuindo para o aprofundamento do debate acadêmico e institucional sobre o tema.

4 RESULTADOS E DISCUSSÕES

A inteligência regulatória digital não pode ser compreendida como mera incorporação instrumental de tecnologias ao campo jurídico, mas como um processo de reconfiguração estrutural da racionalidade regulatória contemporânea. Nesse sentido, a literatura aponta que a digitalização e o uso intensivo de dados transformam a forma como o Direito opera, deslocando seu foco de respostas reativas para modelos baseados na antecipação de riscos e na gestão contínua de comportamentos (Saddy, 2020; Donato et al., 2022).

Esse deslocamento revela uma mudança significativa no papel do Direito Regulatório, que passa a atuar como mecanismo permanente de monitoramento e prevenção. A lógica preditiva, sustentada por algoritmos e análise de grandes volumes de dados, amplia a capacidade de identificação de padrões e comportamentos potencialmente desviantes, permitindo intervenções antes mesmo da ocorrência de infrações propriamente ditas. Conforme destaca Da Cruz (2025), a centralidade dos dados redefine o próprio fundamento da ação regulatória, conferindo maior dinamismo, mas também maior complexidade às decisões jurídicas.

No âmbito das investigações internas corporativas, os resultados indicam que a inteligência regulatória digital altera profundamente a estrutura dos processos investigativos. A substituição de análises pontuais por sistemas contínuos de monitoramento representa avanço significativo em termos de eficiência, sobretudo em ambientes organizacionais complexos (Coutinho, 2018). No entanto, essa transformação não ocorre sem tensões, uma vez que a automatização das decisões desafia a tradição jurídica baseada na reconstrução causal dos fatos (Ferraz Junior, 2021).



Edition: Vol. 02 | N°. 01 | (2026)

Publication: 31/03/2026

DOI: <https://doi.org/10.70579/rfd.v2i1.152>

A opacidade algorítmica emerge, nesse contexto, como um dos principais pontos críticos. A dificuldade de compreender os critérios internos utilizados por sistemas de Inteligência Artificial compromete a transparência das decisões e fragiliza o controle jurídico. Pereira (2021) alerta que decisões baseadas em modelos técnicos pouco acessíveis podem comprometer o dever de motivação, elemento essencial do Estado de Direito, especialmente quando tais decisões produzem efeitos sobre direitos individuais.

Outro resultado relevante refere-se à reconfiguração da noção de responsabilidade jurídica. A fragmentação da cadeia decisória, envolvendo desenvolvedores, operadores, gestores e sistemas automatizados, desafia os modelos clássicos de imputação individual. Nesse cenário, embora a tecnologia participe ativamente da produção das decisões, a responsabilidade permanece necessariamente humana e institucional, sob pena de esvaziamento da accountability (Binenbojm, 2019; Câmara, 2021).

Além disso, a análise evidencia que a incorporação da Inteligência Artificial nas práticas regulatórias intensifica a necessidade de integração entre diferentes campos do Direito. A articulação entre Direito Administrativo, Direito Regulatório, proteção de dados e compliance corporativo torna-se indispensável para assegurar que a eficiência tecnológica não comprometa garantias fundamentais. Aragão (2020) destaca que a governança regulatória contemporânea exige modelos capazes de equilibrar inovação, controle e proteção de direitos, evitando assimetrias de poder decorrentes do uso intensivo de dados.

A análise dos casos institucionais demonstra ainda que a utilização de tecnologias avançadas amplia significativamente a capacidade investigativa. A identificação de padrões complexos, a análise de grandes volumes de dados e a reconstrução de cadeias decisórias tornam-se mais eficientes com o uso de ferramentas digitais (Câmara, 2021). Contudo, como observa Binenbojm (2019), esse ganho de eficiência deve ser acompanhado por mecanismos de controle jurídico que garantam proporcionalidade e legitimidade das intervenções.



Edition: Vol. 02 | Nº. 01 | (2026)

Publication: 31/03/2026

DOI: <https://doi.org/10.70579/rfd.v2i1.152>

Outro ponto relevante refere-se à emergência de novos riscos tecnológicos associados à autonomia dos sistemas de Inteligência Artificial. A evolução para modelos mais autônomos amplia a complexidade dos riscos regulatórios, exigindo modelos de governança mais dinâmicos e adaptativos. Nesse contexto, a antecipação de riscos deixa de se concentrar apenas no comportamento humano, passando a incluir também a análise das dinâmicas algorítmicas (Ijlal, 2025).

Por fim, os resultados indicam que a efetividade da inteligência regulatória digital depende da construção de marcos normativos robustos e da consolidação de uma cultura institucional orientada pela transparência, pela responsabilidade e pela ética. A tecnologia, embora amplie a capacidade regulatória, não substitui a necessidade de fundamentos jurídicos sólidos. Conforme argumentam Donato et al. (2022), a legitimidade da regulação baseada em dados depende da capacidade de submeter esses sistemas aos princípios do Estado de Direito, assegurando equilíbrio entre eficiência e proteção de direitos.

5 CONCLUSÃO

A análise desenvolvida ao longo deste capítulo demonstra que a inteligência regulatória digital representa transformação estrutural na forma como organizações públicas e privadas compreendem, monitoram e respondem a riscos jurídicos em ambientes regulatórios complexos. A convergência entre governança, tecnologia e normatividade evidencia que o Direito contemporâneo deixou de operar exclusivamente por meio de modelos repressivos, incorporando mecanismos preventivos orientados por dados, automação e análise prospectiva.

Os fundamentos do compliance e da governança corporativa permanecem essenciais, mas demandam reinterpretação diante de novos riscos sistêmicos. A consolidação de programas de integridade, a adoção de normas internacionais como a ISO 37001 e a ISO 37301 e sua integração a modelos de Governança, Riscos e



Edition: Vol. 02 | N°. 01 | (2026)

Publication: 31/03/2026

DOI: <https://doi.org/10.70579/rfd.v2i1.152>

Compliance (GRC) demonstram que a prevenção de ilícitos depende de estruturas organizacionais maduras, capazes de articular cultura ética, controles internos e sistemas de gestão robustos.

A complexidade regulatória contemporânea, marcada pela multiplicidade normativa, pela fragmentação institucional e pela centralidade dos dados, exige abordagens dinâmicas de monitoramento normativo. A digitalização amplia a capacidade de identificação de riscos emergentes, mas também introduz desafios relacionados à transparência, à explicabilidade e à imputação de responsabilidade. A literatura especializada alerta que decisões automatizadas não podem comprometer garantias fundamentais, especialmente em contextos investigativos e sancionatórios.

As investigações internas corporativas tornaram-se, nesse cenário, profundamente dependentes de tecnologias forenses, análise de dados e metodologias de inteligência. A prova digital, a análise de vínculos e o uso de ferramentas avançadas de extração e correlação de informações ampliam a capacidade investigativa, mas exigem rigor metodológico, preservação da cadeia de custódia e governança jurídica adequada.

A emergência da *Agentic AI* inaugura, por sua vez, novo paradigma de risco tecnológico. Sistemas autônomos capazes de perceber, raciocinar, agir e aprender de forma contínua ampliam a superfície de ataque, criam vetores de risco e desafiam modelos tradicionais de supervisão humana. Como observa Taimur Ijlal, trata-se de uma IA que “pensa, age e itera”, exigindo salvaguardas jurídicas e técnicas aptas a assegurar *accountability*, proporcionalidade e compatibilidade com o Estado de Direito. (

A inteligência regulatória digital, portanto, não se limita a uma inovação técnica, mas expressa mudança de racionalidade. Sua legitimação depende da construção de marcos normativos robustos, da adoção de sistemas de gestão integrados e da consolidação de uma cultura organizacional orientada pela integridade, pela transparência e pela responsabilidade institucional.

A partir dessa integração entre governança, tecnologia e normatividade, torna-se possível compreender que a inteligência regulatória digital não substitui o Direito, mas o



Edition: Vol. 02 | Nº. 01 | (2026)

Publication: 31/03/2026

DOI: <https://doi.org/10.70579/rfd.v2i1.152>

fortalece, ampliando sua capacidade preventiva, aprimorando sua eficácia e assegurando que a inovação tecnológica permaneça subordinada aos princípios fundamentais do Estado de Direito.

REFERÊNCIAS

ARAGÃO, Alexandre Santos de. **Direito regulatório e políticas públicas**. 3. ed. Rio de Janeiro: Forense, 2020.

BINENBOJM, Gustavo. **Uma teoria do direito administrativo: direitos fundamentais, democracia e constitucionalização**. 3. ed. Rio de Janeiro: Renovar, 2019.

BRASIL. Controladoria-Geral da União (CGU). **Manual prático de programas de integridade**. Brasília: CGU, 2018. Disponível em: <https://repositorio.cgu.gov.br/handle/1/46645>. Acesso em: 2 fev. 2026.

BRASIL. Conselho Administrativo de Defesa Econômica (CADE). **Guia de programas de compliance concorrencial**. Brasília: CADE, 2016. Disponível em: <https://cdn.cade.gov.br/Portal/centrais-de-conteudo/publicacoes/guias-do-cade/guia-compliance-versao-oficial.pdf>. Acesso em: 2 fev. 2026.

CÂMARA, Jacintho Arruda. **Regulação baseada em risco e análise de impacto regulatório**. São Paulo: Malheiros, 2021.

CORIOLOANO, Almeida Camargo; SANTOS, Cleórbete. **Fundamentos do Compliance**. São Paulo: Brasport, 2019.

COUTINHO, Diogo R. **Regulação e democracia: fundamentos jurídicos das políticas públicas**. São Paulo: Saraiva, 2018.

DA CRUZ, Eduardo Otaciano. **Proteção de Dados e Internet das Coisas no Brasil: riscos e soluções na era digital**. São Paulo: Dialética, 2025.

DELFINO LAGROTA ADVOCACIA. **Compliance A–Z: Dicionário**. Kindle Edition, 2026.

DONATO, Thales et al. **A atuação regulatória da Agência Nacional de Proteção de Dados: potencialidades de uma abordagem responsiva**. 2022.

ECHÍCHIQUE. **El eBook Negro sobre la ISO 37001**. Kindle Edition, 2025.

ESSIA, Uwem; EHIWARIO, Kester. **Fundamentals of Governance, Risk Management and Compliance (GRC)**. Kindle Edition, 2026.



Edition: Vol. 02 | Nº. 01 | (2026)
Publication: 31/03/2026
DOI: <https://doi.org/10.70579/rfd.v2i1.152>

- FERRAZ JUNIOR, Tercio Sampaio. **Introdução ao estudo do direito: técnica, decisão e dominação**. 10. ed. São Paulo: Atlas, 2021.
- FIGUEIREDO, Jorge Ramos de; FRANÇA JÚNIOR, Fausto Faustino de. **Extração Forense Avançada de Dados em Dispositivos Móveis**. São Paulo: Brasport, 2022.
- IJLAL, Taimur. **Agentic AI: Navigating Risks and Security Challenges**. 2025.
- JORGE, Higor. **Investigação Criminal Tecnológica**. v. 2. São Paulo: Brasport, 2018.
- MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor**. 2. ed. São Paulo: RT, 2020.
- NJUGUNA, Daniel. **Fraud Examination: Principles, Techniques, and Case Studies**. Kindle Edition, 2025.
- OLIVEIRA, Érick Rodrigues de. **Anticorrupção e Compliance Empresarial**. Kindle Edition, 2025.
- PEREIRA, José Renato Laranjeira de. Transparência pela cooperação: como a regulação responsiva pode auxiliar na promoção de sistemas de *machine learning* inteligentes. **Revista de Direito Setorial e Regulatório**, v. 7, n. 1, p. 194–223, 2021.
- SADDY, André. **Regulação estatal, autorregulação privada e códigos de conduta e boas práticas**. Centro para Estudos Empírico-Jurídicos (CEEJ), 2020.
- SULTAN, Sikander. **Financial Statement Fraud and Detection Strategies**. Great Britain: Expert Of Course, 2021.
- TASSO, Fernando Antonio. **Sistemas Regulatórios de Dados Pessoais**. São Paulo: Editora Foco, 2024.
- YSLA, Alain Casanovas. **Guía práctica de compliance según la Norma ISO 37301**. Kindle Edition, 2021.