GUILHERME
CASELLI

MANUAL DE INVESTIGAÇÃO DIGITAL

5ª edição
revista, atualizada
e ampliada

2026

EDITORA
*Jus*PODIVM
www.editorajuspodivm.com.br

24

RESPONSABILIZAÇÃO DE EMPRESAS DE INTELIGÊNCIA ARTIFICIAL À LUZ DO PARADIGMA DO DIREITO AMBIENTAL

1. INTRODUÇÃO

O avanço da inteligência artificial generativa e dos LLMs, como vimos, introduziu um novo tipo de risco jurídico associado à produção automatizada de informações em escala massiva. Tendo por base falhas associadas às fases de pré-treinamento de grandes modelos de linguagem, os ajustes finos e o aprendizado por reforço a partir do *feedback* humano (RLHF), sistemas dessa natureza podem produzir conteúdos falsos, criminosos, assim como influenciar processos sociais, políticos e econômicos.

Tendo em vista esse paradigma, emerge a necessidade de discutir modelos jurídicos capazes de responsabilizar empresas que desenvolvem e operam tais tecnologias.

Uma hipótese interpretativa relevante consiste em analisar se o regime jurídico ambiental brasileiro, especialmente aquele estruturado pela Lei de Crimes Ambientais (Lei nº 9.605/1998), podendo servir como paradigma normativo para a responsabilização de empresas que operam tecnologias de alto risco.

Por óbvio, esse enfrentamento não pretende realizar analogias utilizáveis na seara do direito penal, mas sim estabelecer nortes jurídicos aptos a lançar luz sobre a necessidade de normatizar e responsabilizar os responsáveis e tomadores de decisões destas *big techs* de IA.

2. INTELIGÊNCIA ARTIFICIAL GENERATIVA E O SURGIMENTO DE NOVOS RISCOS JURÍDICOS

A tutela do Direito Ambiental foi estruturada e construída para lidar com atividades econômicas que produzem riscos difusos e danos coletivos, característica que também se verifica nas tecnologias digitais contemporâneas. Para o avanço desse esboço responsabilizatório, é necessário estabelecer o conceito de dois institutos que começam a eclodir doutrinariamente visando um melhor entendimento do tema. São eles: "Meio Ambiente Digital" e "Ecossistema Informacional".

Meio ambiente digital: surge na doutrina jurídica[1] como extensão do conceito tradicional de meio ambiente. A ideia

1. SANTOS, Samuel Fernandes dos; GOMES, Magno Federici. **A construção de um meio ambiente digital sustentável por meio de políticas públicas de enfrentamento aos riscos cibernéticos.** Seven Editora, 2024. Disponível em: https://sevenpubl.com.br/editora/article/download/6497/11743/25871. Acesso em: 4 mar. 2026

parte da compreensão de que o ambiente humano contemporâneo não é apenas natural ou físico, mas também informacional e tecnológico, ou seja, representa uma dimensão imaterial do meio ambiente que transcende as fronteiras físicas e integra aspectos sociais, econômicos e tecnológicos.

Aqui entende-se por haver o fundamento obrigacional de normatizar o meio ambiente digital, pois, tal instituto corresponde ao ciberespaço enquanto espaço coletivo de circulação de dados, comunicação e interação social, devendo ser protegido juridicamente da mesma forma que o meio ambiente natural. Neste sentido, a difusão das tecnologias informacionais cria um espaço ambiental sujeito a riscos sistêmicos, decorrentes do armazenamento, processamento e disseminação de dados.

Ecossistema informacional: a literatura contemporânea[2] sobre comunicação digital e governança da informação passou a utilizar o conceito de "*information ecosystem*" para descrever o ambiente no qual informações são produzidas, processadas e circulam socialmente.

Nesse sentido, estudos sobre desinformação e governança digital afirmam que ecossistemas informacionais surgem quando indivíduos e instituições utilizam ferramentas tecnológicas para produzir e compartilhar informações em rede e, essas redes são compostas por múltiplos atores sociais, instituições e infraestruturas tecnológicas que estruturam os fluxos de informação.

2. WANLESS, Alicia; LAI, Samantha; HICKS, John. **Assessing National Information Ecosystems.** Carnegie Endowment for International Peace, 2025. Disponível em: https://carnegieendowment.org/research/2025/02/assessing-national-information-ecosystems. Acesso em: 4 mar. 2026.

3. DISTINÇÃO ENTRE MEIO AMBIENTE DIGITAL E ECOSSISTEMA INFORMACIONAL

Poderíamos, então, distinguir os dois institutos da seguinte forma:

Meio Ambiente Digital: o ciberespaço onde ocorrem as interações digitais. Espaço tecnológico e comunicacional formado pela infraestrutura digital, plataformas online e redes de comunicação que possibilitam a interação social, a circulação de dados e a produção de conteúdos no ciberespaço.

Ecossistema Informacional: meio ou forma como as informações circulam e são mediadas dentro desse espaço. É o sistema de relações sociais, tecnológicas e institucionais que organiza a produção, circulação, mediação e consumo de informações dentro do ambiente digital.

4. A ESTRUTURA DE RESPONSABILIZAÇÃO NA LEI DE CRIMES AMBIENTAIS

A Lei de Crimes Ambientais introduziu no ordenamento brasileiro um modelo inovador de responsabilização que rompe com paradigmas clássicos do Direito Penal.

Entre seus principais elementos estruturais destacam-se:

4.1 Responsabilidade penal da pessoa jurídica

A Constituição Federal, em seu art. 225, §3º, passou a admitir expressamente a possibilidade de responsabilização penal de empresas por crimes ambientais, nos seguintes termos:

> "As condutas e atividades consideradas lesivas ao meio ambiente sujeitarão os infratores, pessoas físicas ou jurídicas, a sanções penais e administrativas, independentemente da obrigação de reparar os danos causados."

Por sua vez, a Lei 9.605/1998, lei de crimes ambientais normatizou essa previsão constitucional ao estabelecer, em seu art. 3º:

> "As pessoas jurídicas serão responsabilizadas administrativa, civil e penalmente quando a infração seja cometida por decisão de seu representante legal ou contratual, ou de seu órgão colegiado, no interesse ou benefício da entidade."

Fato é que esse modelo rompe com a tradicional ideia de que apenas pessoas físicas poderiam cometer crimes, permitindo que organizações empresariais sejam responsabilizadas diretamente por danos decorrentes de sua atividade econômica.

Neste sentido, o arcabouço jurídico ambiental aponta algumas possibilidades jurídicas de responsabilização a saber:

I) Responsabilização de dirigentes e administradores - art. 2º da lei 9605/98;

II) Responsabilidade civil objetiva de dirigentes e administradores independe de culpa, baseada no risco da atividade - art. 14, §1º da lei 6.938/1981 — Política Nacional do Meio Ambiente e;

III) Desconsideração da personalidade jurídica – art. 4º — Lei nº 9.605/1998.

4.2 Paralelos Estruturais entre o Direito Ambiental e a Responsabilização por Tecnologias de IA

4.2.1 Empresas de IA como Agentes de Risco Tecnológico

A lógica normativa que fundamenta a responsabilização ambiental baseia-se no seguinte eixo central: atividades que geram risco sistêmico devem assumir responsabilidade ampliada pelos danos decorrentes de sua exploração econômica.

Um substrato comparativo pode ser formulado da seguinte maneira: assim como atividades industriais podem degradar o meio ambiente natural, sistemas algorítmicos têm potencial para degradar o ecossistema informacional.

Esse raciocínio jurídico mostra-se perfeitamente transponível para o campo da inteligência artificial. Empresas que desenvolvem LLMs e outros sistemas de IA operam infraestruturas tecnológicas capazes de produzir impactos amplos sobre o ambiente informacional. Esse paralelo permite a aplicação analógica de alguns fundamentos clássicos do Direito Ambiental:

I. **Atividade de risco**: empresas que exploram sistemas de IA assumem um risco tecnológico funcionalmente semelhante ao risco ambiental.
II. **Externalidades difusas**: os danos decorrentes podem atingir coletividades indeterminadas e de difícil delimitação.
III. **Dificuldade de previsão**: assim como ocorre em acidentes ambientais, os impactos podem apresentar natureza complexa, sistêmica e de difícil antecipação.

Neste cotejo, a difusão de conteúdos nocivos gerados ou amplificados por sistemas tecnológicos — como alucinações

algorítmicas, incitação a comportamentos autodestrutivos, discurso de ódio ou desinformação — pode ser compreendida, por analogia, como uma forma de poluição do ecossistema informacional, pois compromete o ambiente cognitivo coletivo. Assim como a poluição ambiental degrada o meio físico e causa danos difusos, a contaminação do fluxo informacional pode afetar o debate público, a formação da opinião e a qualidade das decisões individuais e coletivas.

4.2.2 A Fase de Aprendizado: "Extrativismo de Dados" sem Licenciamento

No Direito Ambiental, atividades potencialmente lesivas dependem de licenciamento e avaliação prévia de impacto (art. 225, §1º, IV, da Constituição Federal; art. 9º, III e art. 10 da Lei nº 6.938/1981). Por sua vez, em se tratando de LLMs, o ponto crítico situa-se na fase de treinamento dos sistemas de IA.

Por analogia, o treinamento de modelos de IA envolve extração massiva de dados da *web*, muitas vezes obtidos por técnicas de *scraping* (raspagem de dados) em bases abertas que podem conter conteúdos imprecisos ou nocivos. A utilização dessas bases sem curadoria adequada amplia o risco de que tais conteúdos influenciem o comportamento do sistema.

No plano jurídico, essa atividade de extração massiva de dados sem curadoria pode ser analisada sob a lógica do risco da atividade (art. 927, parágrafo único, do Código Civil), aproximando-se da responsabilidade objetiva adotada no Direito Ambiental.

Caso se demonstre que dirigentes tinham ciência dos riscos associados ao uso de bases de dados não curadas, ou seja, com a possibilidade de conter material tóxico e, ainda assim, permitiu o treinamento para acelerar o *time-to-market*,

aceitando o resultado (alucinações perigosas), poderia sugerir um debate jurídico sobre assunção de risco, inclusive sob a perspectiva do dolo eventual no campo penal.

4.2.3 O Dever de Vigilância dos Administradores (Art. 2º da Lei 9605/98)

Outro elemento fundamental previsto na Lei de Crimes Ambientais, que embasa o estudo ora em tela, é a responsabilização de administradores e dirigentes empresariais.

A doutrina reconhece que dirigentes de empresas ocupam posição de garante, devem exercer a vigilância e o controle sobre as atividades da organização empresarial, especialmente quando estas representam fontes potenciais de risco. Neste sentido, o administrador assume o dever jurídico de impedir que a atividade empresarial produza danos a bens jurídicos protegidos, podendo responder penalmente quando, por omissão, deixa de evitar o resultado ilícito.

Aplicando esse raciocínio ao campo da inteligência artificial, pode-se sustentar que executivos e diretores de empresas que desenvolvem e exploram sistemas de IA possuem o dever jurídico de adotar mecanismos mínimos de segurança, governança e controle, especialmente quando a atividade apresenta potencial de gerar riscos difusos ao ambiente informacional.

Nesse contexto, espera-se que as empresas implementem instrumentos técnicos e institucionais destinados a reduzir os riscos associados ao funcionamento desses sistemas, tais como:

I) filtros de conteúdo, voltados à prevenção da geração ou disseminação de material ilícito ou potencialmente lesivo;

II) mecanismos de mitigação de viés, destinados a reduzir distorções discriminatórias decorrentes das bases de treinamento ou do comportamento do modelo;

III) auditorias algorítmicas, capazes de avaliar periodicamente o funcionamento do sistema, seus riscos e eventuais falhas estruturais;

IV) monitoramento de uso abusivo, com mecanismos de detecção e resposta a práticas que possam gerar danos a terceiros.

A adoção dessas medidas integra o conjunto de práticas de governança tecnológica e diligência empresarial, voltadas à gestão de riscos associados ao desenvolvimento e à exploração econômica de sistemas complexos.

Caso tais mecanismos sejam deliberadamente negligenciados pelos tomadores de decisões, especialmente diante do conhecimento prévio dos riscos, pode surgir debate sobre a responsabilidade dos administradores pela produção do dano, em lógica semelhante à aplicada em atividades ambientalmente perigosas. Nessa perspectiva, a omissão consciente na adoção de controles pode ser interpretada como assunção de risco na gestão da atividade, sobretudo quando a empresa possui capacidade técnica para prevenir ou mitigar os danos.

4.2.4 Desconsideração da Personalidade Jurídica

A Lei de Crimes Ambientais trouxe inovação relevante ao estabelecer, em seu art. 4º, a possibilidade de desconsideração da personalidade jurídica quando esta se tornar obstáculo à reparação do dano ambiental. Por meio desse mecanismo, admite-se alcançar diretamente sócios, administradores e controladores, sobretudo quando a estrutura societária é

utilizada para dificultar ou impedir a responsabilização pelos prejuízos causados.

Transposto esse raciocínio para o campo da inteligência artificial, o instituto pode assumir papel particularmente relevante em hipóteses nas quais empresas buscam afastar sua responsabilidade alegando que o comportamento do sistema seria imprevisível, que a tecnologia possuiria autonomia operacional, ou ainda que o resultado danoso decorreu de uma "falha emergente" do modelo.

No entanto, à luz da lógica que orienta o regime jurídico da responsabilidade ambiental, tais argumentos não seriam suficientes, por si sós, para afastar a imputação. Isso porque a atividade econômica que envolve risco relevante permanece juridicamente vinculada aos agentes que a estruturam, a controlam e dela extraem proveito econômico.

Nesse sentido, a invocação de autonomia tecnológica ou de imprevisibilidade do sistema não desloca a responsabilidade para a própria máquina. Ao contrário, reforça a necessidade de identificar quem tomou as decisões de desenvolvimento, treinamento, implementação e disponibilização da tecnologia, bem como quem se beneficia de sua exploração no mercado.

Em última análise, a lógica subjacente permanece a mesma: quem cria e explora uma atividade potencialmente arriscada deve responder pelos efeitos dela decorrentes, especialmente quando dispõe de capacidade técnica e poder decisório para estruturar mecanismos de controle e mitigação de danos.

JUS5463