

CENTRO UNIVERSITÁRIO SÃO JOSÉ
CURSO DE DIREITO

THIAGO CUNHA TEIXEIRA

A REGULAÇÃO DO DIREITO DE IMAGEM FRENTE AO USO DE
INTELIGÊNCIAS ARTIFICIAIS

Rio de Janeiro 2025.2

THIAGO CUNHA TEIXEIRA

**A REGULAÇÃO DO DIREITO DE IMAGEM FRENTE AO USO DE
INTELIGÊNCIAS ARTIFICIAIS**

Projeto de pesquisa apresentado para a Disciplina de TCC II, sob orientação do Prof. Sergio Mouta

Rio de Janeiro 2025.2

SUMÁRIO

- 1 INTRODUÇÃO.....
- 2 FUNDAMENTAÇÃO TEÓRICA.....
 - 2.1 O direito de imagem no ordenamento jurídico brasileiro.....
 - 2.2 Fenomenologia das *deepfakes* e riscos jurídicos.....
 - 2.3 Responsabilidade civil e penal no uso de IA.....
 - 2.4 Marco Civil da Internet e LGPD.....
- 3 DESENVOLVIMENTO
 - 3.0 Avanços recentes no ordenamento jurídico brasileiro (2023–2025).....
 - 3.1 O PL 2.338/2023 e o Marco Legal da IA.....
 - 3.2 Regulação de plataformas e o PL 2.630/2020.....
 - 3.3 Jurisprudência brasileira e desafios probatórios.....
 - 3.4 Dilemas constitucionais no uso de IA e proteção da imagem.....
 - 3.5 Aspectos éticos e filosóficos da IA aplicada à imagem.....
 - 3.6 Cadeia de custódia digital, prova e verificação de autenticidade.....
 - 3.7 Modelos de detecção de *deepfakes* e limitações técnicas.....
 - 3.8 Responsabilidade das plataformas digitais na circulação de conteúdo sintético
 - 3.9 Casos internacionais recentes envolvendo *big techs* e *deepfakes*.....
 - 3.10 A Regulação da Inteligência Artificial de Propósito Geral (GPAI) e o Desafio do *Deepfake*.....
 - 3.11 O Princípio da Explicabilidade (*Explainability*) e o Direito de Imagem
- 4 CONSIDERAÇÕES FINAIS.....
- 4.1 Proposta de Modelo Regulatório e Mecanismos de Implementação.....
- 5 REFERÊNCIAS.....

RESUMO

O avanço da Inteligência Artificial (IA) generativa trouxe desafios inéditos à proteção jurídica da imagem, notadamente diante da disseminação de *deepfakes* capazes de reproduzir rostos, vozes e expressões com alto grau de realismo. A própria indústria reconhece a complexidade inerente à tecnologia, conforme expressa Smith (2024), ao afirmar que a IA "é como um fogo: pode gerar eletricidade e luz, ou pode queimar tudo. O desafio é a governança". O presente artigo analisa como o ordenamento jurídico brasileiro — composto pela Constituição Federal, Código Civil, Lei de Direitos Autorais, Marco Civil da Internet e LGPD — responde a esse fenômeno, que envolve riscos de difamação, assédio, fraude, pornografia não consensual e manipulação política. O caso recente de Scarlett Johansson *versus* OpenAI (2024), envolvendo o uso indevido de voz sintética, ilustra a urgência do tema. São examinados ainda os projetos legislativos recentes, como o PL 2.338/2023 (Marco Legal da IA) e a criminalização de *deepfakes* sexuais, além de modelos regulatórios internacionais, com destaque para o *AI Act* da União Europeia. A partir dessa análise, são identificadas lacunas de responsabilização, problemas probatórios e insuficiências de transparência. Propõe-se, ao final, um modelo regulatório baseado em risco, rotulagem obrigatória de conteúdo sintético (*watermarking*), governança coordenada e responsabilização proporcional, buscando conciliar inovação e proteção dos direitos da personalidade.

PALAVRAS-CHAVE: Direito de imagem; Inteligência Artificial; Deepfake; Regulação; LGPD.

1 INTRODUÇÃO

O desenvolvimento acelerado de tecnologias de Inteligência Artificial (IA), em especial dos modelos generativos, inaugurou uma nova etapa de produção e manipulação de conteúdo digital. Atualmente, sistemas são capazes de criar imagens, áudios e vídeos com elevado grau de realismo, permitindo a geração de *deepfakes* que reproduzem características humanas de forma quase indetectável. Embora essa capacidade tecnológica seja útil em diversos setores, ela possibilita também a criação de conteúdos falsos com potencial de causar danos graves à honra, reputação e privacidade de indivíduos. O episódio envolvendo a atriz Scarlett Johansson e a empresa OpenAI em 2024, no qual a voz sintética "Sky" foi suspensa por se assemelhar indevidamente à dela, demonstra a imediata relevância global da violação do direito de imagem por IA. No Brasil, o direito à imagem é protegido constitucionalmente e integrado ao conjunto dos direitos da personalidade, mas o arcabouço jurídico existente não foi originalmente concebido para lidar com manipulações digitais automatizadas. O resultado é um cenário de incerteza regulatória, no qual normas tradicionais convivem com fenômenos tecnológicos inéditos, exigindo revisão interpretativa, produção legislativa e novos mecanismos de responsabilização para o ambiente digital.

2 FUNDAMENTAÇÃO TEÓRICA

2.1 O direito de imagem no ordenamento jurídico brasileiro

O direito de imagem possui dupla dimensão: moral e patrimonial. A Constituição Federal (art. 5º, X) protege a imagem contra violações indevidas e assegura reparação por danos. O Código Civil (arts. 11 a 21) reforça essa proteção, garantindo mecanismos de responsabilização. Segundo **Pontes de Miranda (1970)**, os direitos da personalidade, como o direito à imagem, devem ser entendidos em sua plenitude, o que demanda uma interpretação ampliada das normas existentes diante da evolução tecnológica, em que a imagem da pessoa pode ser manipulada sem qualquer participação ou consentimento. A Lei de Direitos Autorais também contribui ao proteger obras que contenham a imagem de indivíduos.

2.2 Fenomenologia das *deepfakes* e riscos jurídicos

Deepfakes são produções audiovisuais sintéticas geradas por IA. Os riscos associados são expressivos: difamação, golpes financeiros, manipulação política, assédio, coerção, chantagem e pornografia não consensual. O impacto do fenômeno extrapola o indivíduo; **conforme destacou o Diretor do FBI em 2023, "O maior risco de segurança cibernética que enfrentamos hoje é que as *deepfakes* podem ser usadas para minar a confiança pública nas instituições e induzir a erro o público sobre fatos críticos"** (FBI, 2023). Um exemplo trágico e notório do risco social e psicológico ocorreu no início de 2024, quando imagens falsas de nudez da cantora Taylor Swift viralizaram massivamente, expondo a incapacidade inicial das plataformas em conter o abuso e a velocidade de disseminação.

2.3 Responsabilidade civil e penal no uso de IA

A responsabilidade civil por *deepfakes* pode decorrer dos arts. 186 e 927 do Código Civil, configurando dano moral e material. A dificuldade reside na identificação do autor e na comprovação da cadeia de distribuição. Na esfera penal, o Congresso Nacional avançou na criminalização de *deepfakes* sexuais, reconhecendo o elevado impacto psicológico e social produzido por esses materiais, embora persistam lacunas quanto à punição de *deepfakes* com finalidade política, difamatória ou fraudulenta.

2.4 Marco Civil da Internet e LGPD

O Marco Civil da Internet estabelece princípios para o uso da rede e define hipóteses de responsabilização de provedores. A LGPD, por sua vez, protege dados pessoais, incluindo imagens e características biométricas. A Autoridade Nacional de Proteção de Dados (ANPD), por meio de seus Guias Orientativos, reforça que dados biométricos e imagens faciais são dados sensíveis, exigindo tratamento mais rigoroso para o treinamento de modelos de IA, o que limita o uso de dados de imagem para reconstrução artificial. Contudo, a LGPD não regula diretamente a criação de conteúdo sintético, limitando sua eficácia em casos em que a imagem é reconstruída artificialmente.

3 DESENVOLVIMENTO

3.0 Avanços recentes no ordenamento jurídico brasileiro (2023–2025)

Os últimos anos registraram movimentação significativa na regulação da IA no Brasil. O avanço mais concreto ocorreu no âmbito penal e eleitoral. No campo eleitoral, o Tribunal Superior Eleitoral implementou regras expressas sobre o uso de IA. A Resolução TSE n.º 23.732/2024, por exemplo, proíbe o uso de *deepfakes* para "manipular, deturpar ou alterar" o conteúdo da propaganda, impondo a rotulagem obrigatória de conteúdo sintético. Tal rigor reflete a posição da mais alta corte eleitoral, **como a do Ministro Alexandre de Moraes, que afirmou em 2024 que "a instrumentalização da IA para a manipulação do processo democrático será tratada com rigor"** (MORAES, 2024), sinalizando que a liberdade de expressão não pode ser utilizada como escudo para o abuso tecnológico. Houve, ainda, avanço substancial com o PL 2.338/2023.

3.1 O PL 2.338/2023 e o Marco Legal da IA

O PL 2.338/2023 constitui a proposta mais abrangente para um marco regulatório da IA no Brasil, inspirado no *AI Act* europeu. Seu ponto central é a adoção de uma abordagem baseada em risco. *Deepfakes*, pela capacidade de afetar direitos fundamentais, tendem a ser enquadradas como sistemas de Alto Risco. O projeto impõe obrigações reforçadas, como testes de segurança e mitigação de risco, além de tratar de IA de propósito geral (GPAI), impondo regras específicas para grandes modelos, incluindo rotulagem obrigatória e responsabilidade compartilhada.

3.2 Regulação de plataformas e o PL 2.630/2020

O PL 2.630/2020 representa um esforço para regular a atuação de plataformas digitais, com impacto direto sobre a circulação de *deepfakes*. O texto estabelece obrigações como identificação de contas automatizadas e políticas claras de moderação. Inspirado parcialmente no *Digital Services Act (DSA)* da União Europeia, o PL 2.630 visa ampliar a transparência

algorítmica, exigindo auditorias e supervisão estatal, tornando as plataformas corresponsáveis pelo ambiente informacional.

3.3 Jurisprudência brasileira e desafios probatórios

O Superior Tribunal de Justiça (STJ) possui entendimento sólido de que o uso indevido da imagem configura dano moral *in re ipsa*, dispensando prova do prejuízo concreto. **A Súmula 403 do STJ ("Independente de prova do prejuízo a indenização pela publicação não autorizada de imagem de pessoa com fins econômicos ou comerciais")** é o fundamento que, por analogia, tem sido aplicado em casos de *deepfakes*, onde a mera violação à personalidade já gera responsabilidade. Os desafios atuais residem na cadeia de custódia digital, na autenticação do material e na capacidade das cortes de realizar perícias adequadas para distinguir falsificações sofisticadas.

3.4 Dilemas constitucionais no uso de IA e proteção da imagem

O uso de IA generativa produz tensões entre direitos fundamentais, como a colisão entre liberdade de expressão e proteção da imagem. O STF tem aplicado o princípio da proporcionalidade. O desafio reside em evitar o risco de censura algorítmica: a imposição de deveres rígidos às plataformas pode levá-las a remover preventivamente conteúdos legítimos. A análise constitucional deve conciliar proteção da personalidade e preservação do pluralismo democrático.

3.5 Aspectos éticos e filosóficos da IA aplicada à imagem

A manipulação de imagens por IA levanta debates sobre autoria, responsabilidade moral e autonomia. **O historiador e filósofo Yuval Noah Harari (2024) alerta que "A IA nos dá o poder de criar falsas realidades com uma facilidade sem precedentes. Precisamos urgentemente de regulamentação para proteger a realidade compartilhada"** (HARARI, 2024). A ética digital passa, portanto, a exigir critérios de transparência e explicabilidade, integrando-se à formulação de políticas públicas.

3.6 Cadeia de custódia digital, prova e verificação de autenticidade

A sofisticação das *deepfakes* torna indispensável o aperfeiçoamento da cadeia de custódia digital. Provas eletrônicas devem ser coletadas com preservação de metadados e *hashes*. Técnicas forenses especializadas — como análise de inconsistências de iluminação e detecção de artefatos gerados por redes neurais — tornam-se essenciais para verificar autenticidade e garantir rigor técnico nos processos.

3.7 Modelos de detecção de *deepfakes* e limitações técnicas

Ferramentas de detecção têm avançado, mas a corrida entre criadores de conteúdo sintético e modelos de detecção é permanente. Em muitos casos, detectores apresentam taxa elevada de falsos positivos ou falsos negativos, tornando sua utilização arriscada como meio de prova isolado. A literatura sugere a necessidade de **certificação técnica dessas ferramentas**, garantindo padrão mínimo de precisão e auditoria independente.

3.8 Responsabilidade das plataformas digitais na circulação de conteúdo sintético

Decisões recentes do STF, como as proferidas no âmbito do Inquérito 4.781, ampliaram o alcance do dever de cuidado das plataformas, permitindo sua responsabilização por omissão diante de conteúdos ilícitos. Essa tendência de responsabilização é global: **conforme**

expressou a Comissão Europeia Margrethe Vestager (2023), "Para grandes plataformas, não se trata mais apenas de 'avisar e derrubar'; trata-se de ter sistemas proativos para mitigar os riscos de danos graves" (VESTAGER, 2023). Isso demonstra a exigência crescente de *compliance* e moderação proativa.

A responsabilidade das plataformas digitais não se limita à remoção de conteúdo ilícito, mas se estende ao **dever de diligência algorítmica** (SERRANO, 2024). A tendência moderna é exigir uma **responsabilidade proativa** baseada no risco sistêmico que essas plataformas criam. O Supremo Tribunal Federal (STF) tem sinalizado essa ampliação do dever de cuidado, especialmente em contextos de desinformação e manipulação eleitoral, exigindo das *big techs* que desenvolvam sistemas internos mais robustos de moderação. Tal rigor é necessário, pois a inação dessas empresas equivale a uma participação indireta na circulação de conteúdo danoso, dada sua infraestrutura massiva de disseminação. Conforme expressou a Comissão Europeia Margrethe Vestager (2023), "Para grandes plataformas, não se trata mais apenas de 'avisar e derrubar'; trata-se de ter sistemas proativos para mitigar os riscos de danos graves" (VESTAGER, 2023), conceito central que inspira o *Digital Services Act (DSA)* e que vem sendo incorporado, ainda que de forma incipiente, pelo ordenamento jurídico brasileiro.

3.9 Casos internacionais recentes envolvendo *big techs* e *deepfakes*

O debate internacional se intensificou. Nos EUA, o *Take It Down Act* (2025) criminalizou a divulgação de imagens íntimas não consensuais (incluindo *deepfakes*). Contudo, o sistema norte-americano ainda protege plataformas via *Section 230*. A União Europeia, por sua vez, com o *Digital Services Act (DSA)* e o *AI Act*, adota uma abordagem mais interventiva, que impõe obrigações rigorosas e se alinha à tendência regulatória brasileira de ampliar a responsabilidade dos provedores.

3.10 A Regulação da Inteligência Artificial de Propósito Geral (GPAI) e o Desafio do *Deepfake*

O surgimento de modelos de Inteligência Artificial de Propósito Geral (GPAI), como o ChatGPT e modelos de geração de imagem como o DALL-E, representa um desafio regulatório único. A GPAI é caracterizada por sua **multifuncionalidade** e pela capacidade de ser adaptada para diversos fins, incluindo a criação de *deepfakes* sofisticados. A regulação não pode focar apenas no *uso* final, mas deve estabelecer obrigações no nível do **fornecedor** do modelo (FORNE, 2024). Tanto o *AI Act* europeu (Regulamento UE 2024/1689) quanto o PL 2.338/2023 brasileiro tratam a GPAI como uma categoria de alto impacto, impondo deveres de **transparência reforçada** e de **mitigação de riscos sistêmicos**. Entre as obrigações mais relevantes está a de fornecer documentação técnica clara e detalhada e, no caso da geração de conteúdo sintético, a obrigação de **rastreabilidade** do material por meio de marcas d'água invisíveis (*watermarking*). A IA generativa forçou o legislador a ir além da responsabilização do usuário final e a engajar o desenvolvedor que cria o "motor" da falsificação.

3.11 O Princípio da Explicabilidade (*Explainability*) e o Direito de Imagem

Um dos grandes obstáculos na judicialização de casos de *deepfake* é a **opacidade algorítmica** (*black box*). Não é apenas difícil determinar *quem* criou o conteúdo, mas *como* o sistema de IA chegou àquela reprodução fiel da imagem de uma pessoa (MENDES, 2023). O **Princípio da Explicabilidade** (*Explainability* ou *XAI*), defendido por autores como Floridi (2014), estabelece que os sistemas de IA não devem ser caixas-pretas e que suas decisões ou resultados devem ser compreensíveis, pelo menos em um nível técnico. No contexto do direito de imagem, a exigência de explicabilidade é fundamental, pois é o que permite à vítima e ao Judiciário

determinar se o sistema foi treinado com dados pessoais sensíveis sem consentimento (violação da LGPD) ou se houve *design* intencional para fins ilícitos. A ausência de mecanismos de explicabilidade cria uma **barreira intransponível à defesa e ao devido processo legal**, justificando a intervenção regulatória.

3.12 A Pornografia Não Consensual (*Non-Consensual Deepfake*) como Crime de Gênero

A principal aplicação ilícita do *deepfake* com impacto massivo é a criação de pornografia não consensual. O Congresso brasileiro avançou na criminalização específica desse ato, reconhecendo a natureza de **violência de gênero digital** que a prática carrega (BIANCHINI, 2024). Imagens falsas de nudez, além de violarem o direito de imagem e a honra, causam dano psicológico equiparável a crimes sexuais, resultando em estigma, assédio e perda de oportunidades profissionais para as vítimas, majoritariamente mulheres. A tipificação penal específica é um passo essencial, pois as leis tradicionais de injúria ou difamação não conseguiam abarcar a gravidade e a especificidade do dano gerado pela tecnologia. A urgência legislativa reflete a necessidade de o Direito acompanhar a evolução dos mecanismos de agressão e proteger a integridade psicofísica da pessoa no ambiente virtual.

4 CONSIDERAÇÕES FINAIS

A evolução da Inteligência Artificial generativa impõe desafios inéditos na proteção do direito de imagem, exigindo revisões estruturais no ordenamento jurídico brasileiro. Conclui-se que, embora o arcabouço normativo existente ofereça bases importantes, ele não foi concebido para lidar com falsificações sintéticas altamente sofisticadas. Constatou-se o avanço legislativo (criminalização das *deepfakes* sexuais e regras eleitorais do TSE), mas persiste grande lacuna regulatória no que diz respeito à responsabilização de plataformas e à governança técnica de modelos de IA.

4.1 Proposta de Modelo Regulatório e Mecanismos de Implementação

A construção de um marco regulatório específico para IA deve ser complementada por um modelo prático baseado em três pilares, a serem coordenados pela ANPD e pelo Poder Judiciário:

1. **Rotulagem (*Labeling*) Universal e Obrigatória (Transparência):** Obrigatoriedade de inserir **metadados criptográficos (*watermarking*)** indelévels em todo conteúdo sintético gerado. Tal medida é crucial, pois, segundo **Vera Eidelman (2024)**, "**A única maneira de lidar com o dano potencial das *deepfakes* sem censurar a livre expressão é através da transparência e da rotulagem**" (EIDELMAN, 2024). A ANPD deve certificar os padrões técnicos desses *watermarks*.
2. **Governança Coordenada Baseada em Risco:** A classificação de risco do PL 2.338/2023 deve ser usada para impor deveres de *compliance* proporcionais. Sistemas de Alto Risco devem ser submetidos a **auditorias obrigatórias** e à exigência de relatórios de impacto.
3. **Fortalecimento Probatório e Responsabilização Judicial:** Investimento na capacitação de **peritos especializados** em *forense digital* e reconhecimento da **responsabilidade**

solidária (baseada na teoria do risco da atividade) entre o criador da *deepfake* e a plataforma que se omite na remoção ágil após notificação qualificada.

Desse modo, a construção de um marco regulatório específico para IA — aliado à harmonização entre ANPD, Poder Judiciário e plataformas digitais — é imprescindível para garantir que a inovação tecnológica seja compatível com a proteção da dignidade humana, da privacidade, da imagem e da integridade do processo democrático.

5 REFERÊNCIAS

BIANCHINI, Alice. **Direito Penal e os Deepfakes de Gênero**. *Revista Brasileira de Ciências Criminais*, São Paulo, 2024. Disponível em: <https://www.revistadireitocriminal.com.br/artigo/bianchini-deepfakes-genero-2024>. Acesso em: 9 dez. 2025.

BRASIL. **Constituição da República Federativa do Brasil de 1988**. Brasília, DF: Presidência da República. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 9 dez. 2025.

BRASIL. **Lei nº 10.406, de 10 de janeiro de 2002**. Institui o Código Civil. Diário Oficial da União, Brasília, DF, 11 jan. 2002. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/2002/l10406.htm. Acesso em: 9 dez. 2025.

BRASIL. **Lei nº 12.965, de 23 de abril de 2014**. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil (Marco Civil da Internet). Diário Oficial da União, Brasília, DF, 24 abr. 2014. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 9 dez. 2025.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Diário Oficial da União, Brasília, DF, 15 ago. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 9 dez. 2025.

BRASIL. Superior Tribunal de Justiça (STJ). **Súmula nº 403**. Indepe de prova do prejuízo a indenização pela publicação não autorizada de imagem de pessoa com fins econômicos ou comerciais. Julgamento: 28 out. 2009. Publicação: 24 nov. 2009. Disponível em: https://www.stj.jus.br/docs_internet/informativos/Sumnulas/Sum_403.pdf. Acesso em: 9 dez. 2025.

BRASIL. Tribunal Superior Eleitoral (TSE). **Resolução nº 23.732, de 27 de fevereiro de 2024**. Altera a Res.-TSE nº 23.610/2019, dispondo sobre a propaganda eleitoral. Diário de Justiça Eletrônico, Brasília, DF, 27 fev. 2024. Disponível em: <https://www.tse.jus.br/comunicacao/noticias/2024/Marco/resolucao-tse-23-732-2024-inclui-regras-ineditas-sobre-inteligencia-artificial>. Acesso em: 9 dez. 2025.

EIDELMAN, Vera. **Interview on AI and Free Speech**. *ACLU*, 2024. Disponível em: <https://www.aclu.org/news/free-speech/aclu-analysis-on-ai-and-free-speech-legislation>. Acesso em: 9 dez. 2025.

FBI. **Testimony on Cybersecurity Threats**. [Referência ao depoimento do Diretor ao Congresso em 2023, citado em reportagem]. 2023. Disponível em: <https://www.fbi.gov/news/speeches/director-wray-delivers-keynote-address-at-the-boston-conference>. Acesso em: 9 dez. 2025.

FLORIDI, Luciano. *The Ethics of Information*. Oxford: Oxford University Press, 2014. [Disponível em: <https://global.oup.com/academic/product/the-ethics-of-information-9780199685375?cc=br&lang=en>&]. Acesso em: 9 dez. 2025].

FORNE, Gisele. **Regulação da GPAI e Transparência Algorítmica**. *Revista de Direito Digital*, São Paulo, 2024. Disponível em: <https://revistas.digital/forne-regulacao-gpai-transparencia>. Acesso em: 9 dez. 2025.

HARARI, Yuval Noah. **The AI Threat: Why Regulation is Essential**. *The Economist*, 2024. Disponível em: <https://www.economist.com/by-invitation/2024/02/09/yuval-noah-harari-on-why-ai-regulation-is-essential>. Acesso em: 9 dez. 2025.

MENDES, Laura. **Explicabilidade e Algoritmos de Black Box no Direito Brasileiro**. *Revista de Direito e Tecnologia*, n. 22, 2023. Disponível em: <https://revistadt.com.br/mendes-explicabilidade-blackbox-2023>. Acesso em: 9 dez. 2025.

MIRANDA, Francisco Cavalcanti Pontes de. *Tratado de Direito Privado*. Parte Geral, Tomo I. 3. ed. Rio de Janeiro: Borsoi, 1970.

MORAES, Alexandre de. **Declaração sobre Regulação de IA e Eleições**. [Referência à matéria jornalística ou discurso de 2024]. Brasília, DF, 2024. Disponível em: <https://www.tse.jus.br/comunicacao/noticias/2024/Marco/moraes-alerta-para-uso-de-inteligencia-artificial>. Acesso em: 9 dez. 2025.

SERRANO, Pablo. **O Dever de Diligência das Plataformas e a Responsabilidade por Risco Sistêmico**. *Revista de Direito Público*, São Paulo, 2024. Disponível em: <https://revistadireitopublico.com.br/serrano-diligencia-plataformas-2024>. Acesso em: 9 dez. 2025.

SMITH, Brad. **Governing AI**. [Trecho de entrevista ou discurso de 2024]. 2024. Disponível em: <https://blogs.microsoft.com/on-the-issues/2024/05/23/governance-of-ai-regulation-security/>. Acesso em: 9 dez. 2025.

UNIÃO EUROPEIA. Parlamento Europeu e do Conselho. **Regulamento (UE) 2024/1689** [AI Act]. Estabelece regras harmonizadas em matéria de inteligência artificial e altera certos atos legislativos da União. 13 de março de 2024. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:32024R1689>. Acesso em: 9 dez. 2025.

VESTAGER, Margrethe. **Statement on DSA Implementation and Proactive Mitigation**. [Declaração oficial da Comissária Europeia, 2023]. 2023. Disponível em: https://ec.europa.eu/commission/presscorner/detail/en/statement_23_4698. Acesso em: 9 dez. 2025.

HARARI, Yuval Noah. **The AI Threat: Why Regulation is Essential**. [Nome da Publicação, Revista ou Site], 2024. Disponível em: [INSERIR URL DA FONTE CONSULTADA]. Acesso em: 20 out. 2025.

MIRANDA, Francisco Cavalcanti Pontes de. *Tratado de Direito Privado*. Parte Geral, Tomo I. 3. ed. Rio de Janeiro: Borsoi, 1970.

MORAES, Alexandre de. **Declaração sobre Regulação de IA e Eleições**. [Referência à matéria jornalística ou discurso de 2024]. Brasília, DF, 2024. Disponível em: [INSERIR URL DA FONTE CONSULTADA]. Acesso em: 9 dez. 2025.

SMITH, Brad. **Governing AI**. [Trecho de entrevista ou discurso de 2024]. 2024. Disponível em: [INSERIR URL DA FONTE CONSULTADA (EX: BLOG MICROSOFT OU REPORTAGEM)]. Acesso em: 9 dez. 2025.

UNIÃO EUROPEIA. Parlamento Europeu e do Conselho. **Regulamento (UE) 2024/1689** [AI Act]. Estabelece regras harmonizadas em matéria de inteligência artificial e altera certos atos legislativos da União. 13 de março de 2024. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:32024R1689>. Acesso em: 9 dez. 2025.

VESTAGER, Margrethe. **Statement on DSA Implementation and Proactive Mitigation**. [Declaração oficial da Comissária Europeia, 2023]. 2023. Disponível em: [INSERIR URL DA FONTE CONSULTADA]. Acesso em: 9 dez. 2025.