doi.org/10.51891/rease.v12i11.33312

CONTROLE DE CONVENCIONALIDADE E USO ESTATAL DE INTELIGÊNCIA ARTIFICIAL DE ALTO RISCO: PARÂMETROS INTERAMERICANOS E A CONTRIBUIÇÃO COMPARATIVA DO EU AI ACT

CONVENTIONALITY CONTROL AND STATE USE OF HIGH-RISK ARTIFICIAL INTELLIGENCE: INTER-AMERICAN STANDARDS AND THE COMPARATIVE CONTRIBUTION OF THE EU AI ACT

CONTROL DE CONVENCIONALIDAD Y USO ESTATAL DE INTELIGENCIA ARTIFICIAL DE ALTO RIESGO: PARÁMETROS INTERAMERICANOS Y LA CONTRIBUCIÓN COMPARATIVA DEL EU AI ACT

Carlos Eduardo Chaves[1]
Graziela Tavares de Souza Reis[2]

RESUMO: Esse artigo buscou analisar em que medida o controle de convencionalidade pode funcionar como parâmetro jurídico para avaliar e limitar a utilização de sistemas de inteligência artificial de alto risco pelo Estado brasileiro, à luz das obrigações do Sistema Interamericano de Direitos Humanos, tendo o Regulamento (UE) 2024/1689 (EU AI Act) como referência comparativa. Adotou-se o método hipotético-dedutivo, com abordagem qualitativa e procedimentos bibliográficos e documentais. Os resultados indicam que os riscos da inteligência artificial estatal, como vieses e discriminação algorítmica, opacidade, falhas de segurança, desinformação e uso indevido de dados, atingem direitos protegidos pela Convenção Americana sobre Direitos Humanos, para os quais a jurisprudência da Corte Interamericana oferece parâmetros aplicáveis, e que o regime europeu, embora útil, tem natureza predominantemente regulatória e comporta exceções na atuação estatal mais sensível. O exame do reconhecimento facial na segurança pública apontou indício de déficit de legalidade no Brasil. Conclui-se que a hipótese se confirma com ressalvas: o controle de convencionalidade é parâmetro juridicamente consistente, mas sua eficácia depende do exercício preventivo por todas as autoridades, de critérios concretos, para os quais o EU AI Act contribui sem força vinculante, e de condições institucionais de transparência, capacidade técnica e responsabilização.

Palavras-chave: Controle de convencionalidade. Inteligência artificial. Sistema Interamericano de Direitos Humanos.

ABSTRACT: This article analyzed the extent to which conventionality control can serve as a legal standard for assessing and limiting the use of high-risk artificial intelligence systems by the Brazilian State, in light of the obligations of the Inter-American Human Rights System, with Regulation (EU) 2024/1689 (EU AI Act) as a comparative reference. The hypothetical-deductive method was adopted, with a qualitative approach and bibliographic and documentary procedures. The results indicate that the risks of state artificial intelligence, such as algorithmic bias and discrimination, opacity, security failures, disinformation and misuse of data, affect rights protected by the American Convention on Human Rights, for which Inter-American case law provides applicable standards, and that the European regime, although useful, is predominantly regulatory in nature and admits exceptions in the most sensitive state activities. The examination of facial recognition in public security indicated a legality deficit in Brazil. The hypothesis is confirmed with reservations: conventionality control is a legally consistent standard, but its effectiveness depends on preventive exercise by all authorities, on concrete

[1] Graduando em Direito. Universidade Federal do Tocantins (UFT), Câmpus de Palmas.
[2] Orientadora. Advogada. Doutora em Integração da América Latina pela Universidade de São Paulo (USP). Professora Adjunta do curso de Direito da Universidade Federal do Tocantins (UFT), Câmpus de Palmas.

criteria, to which the EU AI Act contributes without binding force, and on institutional conditions of transparency, technical capacity and accountability.

Keywords: Conventionality control. Artificial intelligence. Inter-American Human Rights System.

RESUMEN: Este artículo analizó en qué medida el control de convencionalidad puede funcionar como parámetro jurídico para evaluar y limitar el uso de sistemas de inteligencia artificial de alto riesgo por el Estado brasileño, a la luz de las obligaciones del Sistema Interamericano de Derechos Humanos, con el Reglamento (UE) 2024/1689 (EU AI Act) como referencia comparativa. Se adoptó el método hipotético-deductivo, con enfoque cualitativo y procedimientos bibliográficos y documentales. Los resultados indican que los riesgos de la inteligencia artificial estatal, como sesgos y discriminación algorítmica, opacidad, fallas de seguridad, desinformación y uso indebido de datos, afectan derechos protegidos por la Convención Americana sobre Derechos Humanos, para los cuales la jurisprudencia interamericana ofrece parámetros aplicables, y que el régimen europeo, aunque útil, tiene naturaleza predominantemente regulatoria y admite excepciones en la actuación estatal más sensible. El examen del reconocimiento facial en la seguridad pública señaló un déficit de legalidad en Brasil. La hipótesis se confirma con reservas: el control de convencionalidad es un parámetro jurídicamente consistente, pero su eficacia depende del ejercicio preventivo por todas las autoridades, de criterios concretos, a los que contribuye el EU AI Act sin fuerza vinculante, y de condiciones institucionales de transparencia, capacidad técnica y rendición de cuentas.

Palabras clave: Control de convencionalidad. Inteligencia artificial. Sistema Interamericano de Derechos Humanos.

1 INTRODUÇÃO

A incorporação de sistemas de inteligência artificial (IA) às atividades estatais deixou de ser uma hipótese: tribunais, forças de segurança, administrações penitenciárias e outros órgãos públicos passaram a empregar ferramentas automatizadas para classificar processos, identificar pessoas, estimar riscos e subsidiar decisões. Essas aplicações prometem eficiência, mas transferem para modelos estatísticos parte de juízos que repercutem sobre a liberdade, a igualdade, a privacidade e o acesso à justiça. Quando o usuário é o próprio Estado, as falhas desses sistemas deixam de ser um problema apenas técnico e passam a afetar direitos assegurados pela Constituição Federal e pela Convenção Americana sobre Direitos Humanos (CADH).

Os riscos, contudo, não se distribuem de modo uniforme. Os sistemas de alto risco, por sua aptidão para interferir em decisões que afetam a liberdade, a igualdade, o devido processo e a não discriminação, exigem regime jurídico qualificado, e é sobre essa categoria que recai o presente estudo. A delimitação toma como referência o Regulamento (UE) 2024/1689, conhecido como *Artificial Intelligence Act* (EU AI Act), do qual se analisa apenas o regime aplicável aos sistemas de alto risco e os limites de sua utilização como referência para o Brasil.

No continente americano, inexiste regulação regional equivalente, e o Brasil ainda não dispõe de lei específica em vigor sobre IA. A ausência de um marco normativo específico não implica, todavia, ausência de parâmetros jurídicos aplicáveis: o Brasil é Estado parte da CADH, reconhece a jurisdição contenciosa da Corte Interamericana de Direitos Humanos (Corte IDH) e está sujeito ao dever de controle de convencionalidade, por meio do qual os órgãos estatais, no âmbito de suas competências, devem verificar a compatibilidade dos atos internos com a Convenção e com a interpretação que dela faz a Corte IDH.

Diante desse quadro, formula-se o seguinte problema de pesquisa: em que medida o controle de convencionalidade pode funcionar como parâmetro jurídico para avaliar e limitar a utilização de sistemas de inteligência artificial de alto risco pelo Estado brasileiro, à luz das obrigações assumidas no âmbito do Sistema Interamericano de Direitos Humanos (SIDH), utilizando o EU AI Act como referência comparativa?

O objetivo geral é analisar se, e em que condições, o controle de convencionalidade pode servir de parâmetro para avaliar e limitar o uso estatal de sistemas de IA de alto risco. Como objetivos específicos, busca-se: identificar os riscos jurídicos da utilização desses sistemas pelo Estado e correlacioná-los com os direitos protegidos pela CADH e com a jurisprudência da Corte IDH; examinar o regime europeu dos sistemas de alto risco e os limites de seu uso como referência; e verificar como o controle de convencionalidade pode ser aplicado a esses usos no ordenamento brasileiro.

A pesquisa justifica-se pela relevância prática do tema, pois decisões estatais apoiadas por IA podem atingir direitos de forma ampla e pouco visível, e pela necessidade de examinar o que um mecanismo já disponível no ordenamento brasileiro pode oferecer (e o que não pode) diante desses usos.

Adotou-se o método hipotético-dedutivo, partindo da hipótese de que o controle de convencionalidade constitui instrumento apto a controlar a utilização estatal de sistemas de IA de alto risco, tendo como parâmetro as obrigações decorrentes da CADH e da jurisprudência interamericana, ao passo que as obrigações do EU AI Act podem funcionar como elementos interpretativos para a concretização desses parâmetros, sem constituir obrigação convencional para o Estado brasileiro. A pesquisa, qualitativa, exploratória e explicativa, valeu-se de procedimentos bibliográficos e documentais, com exame da legislação europeia e brasileira, de tratados interamericanos, da jurisprudência da Corte IDH e de documentos da Comissão

Interamericana de Direitos Humanos (CIDH) e da Organização dos Estados Americanos (OEA).

2 O SISTEMA INTERAMERICANO DE DIREITOS HUMANOS E OS SISTEMAS DE IA DE ALTO RISCO

O Sistema Interamericano de Direitos Humanos (SIDH) é o sistema regional de proteção dos direitos humanos estruturado no âmbito da Organização dos Estados Americanos (OEA). A CADH, que entrou em vigor apenas em 1978, tornou-se o principal instrumento do sistema por sua abrangência geográfica, por seu catálogo de direitos civis e políticos e por instituir um mecanismo de supervisão e controle das obrigações estatais que inclui um tribunal internacional (Ramos, 2009, p. 248). Esse mecanismo apoia-se em dois órgãos: a CIDH, que promove o respeito aos direitos, recebe petições de vítimas, recomenda condutas aos Estados e pode submeter casos à Corte; e a Corte IDH, que julga a responsabilidade internacional dos Estados (Ramos, 2009, p. 249-251) e exerce, ainda, função consultiva.

O Brasil vincula-se ao sistema por ato próprio. Ratificou a CADH, promulgada pelo Decreto nº 678/1992 (Brasil, 1992), e, em 10 de dezembro de 1998, reconheceu a jurisdição obrigatória da Corte IDH, reconhecimento promulgado internamente pelo Decreto nº 4.463/2002 (Brasil, 2002). Com isso, comprometeu-se a respeitar e garantir os direitos convencionais sem discriminação (Brasil, 1992, art. 1.1) e a cumprir as decisões da Corte nos casos em que for parte (Brasil, 1992, art. 68.1). No sistema interamericano, essas decisões devem ser cumpridas integralmente, e o Estado não pode alegar impedimentos de direito interno para descumpri-las (Ramos, 2009, p. 251-252; Brasil, 2009b, art. 27). Para o direito internacional, ademais, o Estado federal é uno e responde internacionalmente mesmo quando o ilícito decorre de atribuição de um ente federado (Ramos, 2009, p. 276), aspecto relevante para esta pesquisa, pois parte dos usos estatais de IA na segurança pública, como o reconhecimento facial, é promovida por governos estaduais.

A importância do SIDH reside na articulação entre um catálogo de direitos e processos internacionais que interpretam seu conteúdo e fiscalizam seu cumprimento. Como observam Ramos e Gama (2022, p. 286), no direito internacional dos direitos humanos os Estados assumem deveres em prol dos indivíduos, sem a lógica de reciprocidade dos tratados tradicionais, e as pessoas têm acesso a instâncias internacionais de supervisão. Por isso, não basta reconhecer formalmente os direitos convencionais: não cabe interpretar a CADH sob uma ótica nacional, desprezando a interpretação da Corte IDH, sob pena de se criar o que os autores denominam

"tratado internacional nacional" (Ramos; Gama, 2022, p. 287-289). Para o objeto desta pesquisa, essa importância é ainda maior, pois, diante da inexistência de regulação regional específica sobre IA e de lei brasileira em vigor sobre a matéria, o SIDH oferece o principal conjunto de parâmetros jurídicos regionais vinculantes de que se dispõe para avaliar o uso estatal de sistemas de alto risco.

2.1 A proteção dos direitos humanos diante das novas tecnologias no SIDH

O ponto de partida é a distinção entre as fontes do sistema segundo sua força jurídica, uma vez que no plano vinculante, situam-se a CADH e os demais tratados interamericanos ratificados pelo Brasil, como a Convenção Interamericana para Prevenir, Punir e Erradicar a Violência contra a Mulher (Convenção de Belém do Pará) (Brasil, 1996) e a Convenção Interamericana contra o Racismo, a Discriminação Racial e Formas Correlatas de Intolerância, esta equivalente às emendas constitucionais por ter sido aprovada pelo rito do art. 5º, § 3º, da Constituição (Brasil, 2022a; Ramos; Gama, 2022, p. 288), bem como as sentenças da Corte IDH nos casos em que o Brasil for parte (Brasil, 1992, art. 68.1). A jurisprudência da Corte em outros casos e em opiniões consultivas, embora não produza condenação do Estado, expressa a interpretação autorizada da Convenção, que as autoridades nacionais devem considerar no controle de convencionalidade (Corte IDH, 2009c, § 339; Corte IDH, 2014c, § 31). Por fim, os informes da CIDH, as declarações de relatores especiais e os princípios do Comitê Jurídico Interamericano têm natureza orientativa: não criam obrigações autônomas, mas auxiliam a interpretá-las.

Três obrigações gerais estruturam a proteção. A primeira é a de respeitar e garantir os direitos sem discriminação (Brasil, 1992, art. 1.1). Desde seu primeiro caso contencioso, a Corte IDH afirma que o dever de garantia implica organizar todo o aparato governamental de modo a assegurar juridicamente o livre e pleno exercício dos direitos, prevenindo, investigando e sancionando suas violações (Corte IDH, 1988, § 166), e que o Estado pode ser responsabilizado por atos de particulares quando deixa de agir com a devida diligência para preveni-los (Corte IDH, 1988, § 172-175). A segunda é a de adotar disposições de direito interno, legislativas ou de outra natureza, necessárias para tornar efetivos os direitos (Brasil, 1992, art. 2º). A terceira é a de reparar as violações (Brasil, 1992, art. 63.1).

Essas obrigações alcançam a atuação de particulares que prestam serviços em nome do Estado, que deve regulá-los e fiscalizá-los permanentemente, como afirmado em *Ximenes Lopes*

vs. Brasil (Corte IDH, 2006c, § 98-99), e exigir das empresas devida diligência em direitos humanos, como afirmado em *Los Buzos Miskitos vs. Honduras* (Corte IDH, 2021b). Essa linha é decisiva para o problema da indefinição de responsabilidades: a contratação de sistema desenvolvido por empresa privada não afasta a responsabilidade internacional do Estado que o utiliza, nem o dever de regular e fiscalizar seu funcionamento.

A ausência de previsão expressa sobre inteligência artificial na CADH não constitui obstáculo. A Corte IDH reiteradamente afirma que os tratados de direitos humanos são instrumentos vivos, cuja interpretação deve acompanhar a evolução dos tempos e as condições de vida atuais (Corte IDH, 1999, § 114), o que permite aplicar a novas tecnologias as garantias já consagradas.

No plano orientativo, há standards da Relatoria Especial para a Liberdade de Expressão da CIDH sobre a internet (CIDH, 2013; 2017), princípios atualizados do Comitê Jurídico Interamericano sobre proteção de dados (OEA, 2021) e declaração conjunta de relatores especiais, de 2025, sobre IA e liberdade de expressão (Nações Unidas *et al.*, 2025), mas não se identificou decisão contenciosa da Corte IDH dedicada especificamente a sistemas de IA, o que confere especial importância à tarefa de extrair, da jurisprudência existente, os parâmetros aplicáveis.

2.2 Correlação entre os riscos da IA estatal e os direitos protegidos pela CADH

Quando o usuário da IA é o Estado, os riscos adquirem contornos próprios, por três razões. Em primeiro lugar, o Estado atua com poder de império: a pessoa submetida a uma decisão administrativa ou judicial apoiada por IA, em regra, não pode recusar o sistema nem escolher outro fornecedor. Em segundo lugar, há assimetria de informação e de poder entre a autoridade que utiliza a ferramenta e o indivíduo afetado, assimetria que o próprio EU AI Act reconhece como critério para a identificação de usos de alto risco (União Europeia, 2024, art. 7º, n. 2). Em terceiro lugar, o Estado é o destinatário direto das obrigações de respeito e garantia dos direitos humanos assumidas no SIDH (Brasil, 1992, art. 1.1), razão pela qual o dano produzido por um sistema estatal de IA pode configurar não apenas um ilícito interno, mas também um fato gerador de responsabilidade internacional. Os riscos examinados a seguir atravessam as categorias de riscos operacionais, de interação e sistêmicos propostas por Braga e Perez Filho (2025, p. 8), mas não são tratados com a mesma profundidade: privilegiam-se aqueles

mais diretamente relacionados ao uso estatal de sistemas que interferem em decisões sobre direitos

A correlação parte de cada um desses riscos para localizar o direito convencional afetado e o parâmetro interamericano que o protege. O risco tecnológico não equivale, por si só, a violação convencional: a incompatibilidade com a CADH surge quando o uso do sistema carece de base legal, persegue finalidade ilegítima, impõe restrições desnecessárias ou desproporcionais, produz efeitos discriminatórios, impede a contestação das decisões ou quando o Estado deixa de adotar a prevenção razoavelmente exigível diante de riscos que conhecia ou deveria conhecer. É nesse último ponto, o da devida diligência, que as salvaguardas europeias têm maior utilidade comparativa.

2.2.1 Igualdade e não discriminação (arts. 1.1 e 24 da CADH)

Os sistemas de aprendizado de máquina são treinados sobre dados que expressam comportamentos humanos passados e presentes, marcados por vieses e preconceitos determinados por circunstâncias históricas, culturais e sociais, por essa razão, tendem a reproduzir estruturas atuais e pretéritas de inclusão e exclusão (Barroso; Mello, 2024, p. 22). Cavalcante (2023, p. 16) aponta como causas principais do viés algorítmico a estrutura social preexistente, os dados enviesados, a construção da ferramenta e a interpretação dos resultados, concluindo que, por maior que seja a confiança depositada no *big data*, sistemas inteligentes poderão ser discriminatórios. Crestane (2023, p. 14-15) define a discriminação algorítmica como a negativa automatizada de acesso a bem, direito ou serviço com base em inferência algorítmica equivocada ou enviesada, forma de reprodução da discriminação estrutural que incide sobre a igualdade de modo dificilmente perceptível pela vítima.

O problema não se resolve com a exclusão de variáveis sensíveis: mesmo bases aparentemente neutras carregam desigualdades sistêmicas, e o cruzamento de informações como raça, gênero ou classe social pode gerar perfis discriminatórios sem intenção de discriminar (Ferrari; Becker; Wolkart, 2018 *apud* Velloso; Consalter, 2025, p. 7).

Os exemplos de uso estatal são significativos, nos Estados Unidos, o *software* Correctional Offender Management Profiling for Alternative Sanctions (COMPAS), utilizado para estimar o risco de reincidência, atribuía a réus negros, segundo análise da ProPublica, chances 45% maiores de receber pontuações elevadas do que a réus brancos com características semelhantes (Sauthier, 2026, p. 13-14). No Brasil, levantamento da Rede de Observatórios da

Segurança apontou que 90,5% das 151 pessoas presas com uso de reconhecimento facial entre junho e outubro de 2019 eram negras (Oliveira, 2019), e episódio de detenção indevida de um torcedor em estádio de futebol levou o Estado de Sergipe a suspender a utilização da ferramenta (Barroso; Mello, 2024, p. 22-23).

Alguns fatores agravam esse risco quando o usuário é o Estado: a escala, pois um erro que afetaria um caso passa a afetar milhares (Cavalcante, 2023, p. 74-75), a opacidade, pois, diante de modelos que funcionam como "caixas-pretas", a pessoa afetada não conhece as razões do tratamento recebido e tem dificuldade para contestá-lo (Sauthier, 2026, p. 11) e a legitimação, pois o problema deixa de ser a mera reprodução de preconceitos e passa a ser sua institucionalização em políticas aparentemente legais (Velloso; Consalter, 2025, p. 8).

A discriminação de gênero segue o mesmo mecanismo, como mostra o sistema de recrutamento da Amazon, abandonado por preferir candidatos homens (Barroso; Mello, 2024, p. 22). A interseção entre raça e gênero agrava o problema, Reis (2026, p. 543), com base no estudo *Gender Shades*, relata que os três sistemas comerciais de classificação de gênero por análise facial avaliados tiveram o pior desempenho no grupo de mulheres de pele escura, com taxas de erro de até 34,7%, enquanto homens de pele clara apresentaram taxas próximas de zero. No âmbito estatal, esses vieses podem atingir a seleção de servidores, a concessão de benefícios e as avaliações de risco em casos de violência doméstica, o que os conecta às obrigações de prevenção da violência contra a mulher examinadas a seguir.

Na CADH, o art. 1.1 proíbe a discriminação no gozo dos direitos convencionais, e o art. 24 assegura a igual proteção da lei (Corte IDH, 2012, § 82). O princípio integra o *jus cogens* (Corte IDH, 2003, § 101), veda a discriminação direta ou indireta, de jure ou de fato (Corte IDH, 2015, § 173), e exige medidas positivas para revertê-la (Corte IDH, 2020a, § 89). A Convenção Interamericana contra o Racismo, com hierarquia constitucional no Brasil, define a discriminação racial pelo propósito ou efeito de restringir direitos e alcança a discriminação indireta produzida por critério aparentemente neutro (Brasil, 2022a, art. 1.1 e 1.2), formulação que se ajusta à discriminação algorítmica, que raramente decorre de intenção declarada.

No policiamento automatizado, aplica-se o entendimento firmado em *Fernández Prieto y Tumbeiro vs. Argentina*, segundo o qual detenções fundadas em estereótipos supõem presunção de culpabilidade e são arbitrárias, exigindo-se fatos concretos e suficientes para restringir a liberdade (Corte IDH, 2020c). Uma suspeita gerada por reconhecimento facial com taxas de erro desiguais conforme a raça pode reproduzir essa lógica sob aparência técnica. Quanto ao

gênero, a Convenção de Belém do Pará impõe ao Estado a devida diligência na prevenção da violência e a modificação de padrões socioculturais estereotipados (Brasil, 1996, arts. 6º, *b*, 7º, *b*, e 8º, *b*). Para Reis (2026, p. 547), essa definição de violência "deve ser interpretada de forma evolutiva, considerando que a violência de gênero pode ser mediada por tecnologias digitais", razão pela qual o Estado não pode permanecer passivo diante de sistemas que reproduzem discriminações de gênero ou produzem riscos previsíveis, cabendo-lhe adotar regulação, fiscalização, avaliação de impacto, transparência e mecanismos de reparação. A Corte IDH define o estereótipo de gênero como a preconcepção de atributos ou papéis de homens e mulheres (Corte IDH, 2009b, § 401) e já reconheceu, em caso contra o Brasil, a discriminação interseccional de mulheres e meninas afrodescendentes em situação de pobreza (Corte IDH, 2020b, § 200), parâmetros aplicáveis aos usos estatais referidos acima.

2.2.2 Vida privada, honra e dignidade (art. 11 da CADH) e autodeterminação informativa

Entre os riscos à privacidade, Barroso e Mello (2024, p. 21-22) destacam a vigilância e o rastreamento por governos e autoridades policiais mediante reconhecimento facial e ferramentas de localização, cujos riscos de abuso "são muito grandes", e os vazamentos decorrentes das vastas bases de dados necessárias ao treinamento dos modelos.

No Brasil, a proteção de dados pessoais foi reconhecida como direito fundamental autônomo, inclusive nos meios digitais (Brasil, 2020; 2022b). Subsiste, contudo, uma lacuna relevante: a Lei Geral de Proteção de Dados (LGPD) não se aplica ao tratamento de dados realizado para fins exclusivos de segurança pública, defesa nacional, segurança do Estado ou atividades de investigação e repressão de infrações penais, que devem ser regidos por legislação específica (Brasil, 2018, art. 4º, III, e § 1º), ainda não editada. É justamente nesse campo que se concentram alguns dos usos estatais de IA mais intrusivos, como o reconhecimento facial em espaços públicos.

A vigilância estatal e o uso indevido de dados atingem a vida privada. A CADH protege a vida privada contra ingerências arbitrárias ou abusivas (Brasil, 1992, art. 11.2 e 11.3), e a Corte IDH, em *Escher y otros vs. Brasil*, estendeu essa proteção aos dados de origem, destino, frequência e duração das comunicações, exigindo que as ingerências estejam previstas em lei, persigam fim legítimo e sejam idôneas, necessárias e proporcionais (Corte IDH, 2009a, § 114-116). Em *Miembros de la Corporación Colectivo de Abogados "José Alvear Restrepo" vs. Colombia* (CAJAR), de 2023, a Corte reconheceu a autodeterminação informativa como direito autônomo, exigiu lei em

sentido formal para as atividades de inteligência, considerou incompatíveis interceptações e requisições de dados sem controle judicial e declarou violado o art. 2º em relação aos arts. 11.2 e 13.1, diante da inadequação da legislação colombiana (Corte IDH, 2023).

2.2.3 Garantias judiciais e proteção judicial (arts. 8 e 25 da CADH)

A opacidade das decisões apoiadas por IA, que impede a pessoa de conhecer os critérios utilizados e de contestar o resultado, atinge as garantias judiciais e a proteção judicial. Na CADH, as garantias do art. 8.1 vinculam qualquer autoridade que determine direitos e obrigações (Corte IDH, 2001, § 71), inclusive o dever de motivação, que assegura o direito de ser julgado pelas razões que o direito fornece (Corte IDH, 2008, § 77-78), e o art. 25 garante recurso simples, rápido e efetivo, ambos violados em *Fernández Prieto y Tumbeiro* (Corte IDH, 2020c). Como mostra o COMPAS, sem conhecer os cálculos e as correlações do sistema, o acusado não dispõe de ampla defesa (Cavalcante, 2023, p. 81-82), de modo que a opacidade algorítmica pode ser tratada como déficit de fundamentação e de contestabilidade.

Em matéria penal e sancionatória, o *standard* interamericano é especialmente exigente: a pessoa deve poder conhecer e impugnar os elementos que influíram na decisão, e a autoridade deve demonstrar ter formado convicção própria. No Brasil, a Resolução nº 615/2025 do Conselho Nacional de Justiça (CNJ) converge com essa orientação ao vedar soluções que não possibilitem revisão humana ou que valorem traços de personalidade para prever crimes ou reiteração delitiva (CNJ, 2025, art. 10, I e II; Velloso; Consalter, 2025, p. 12).

2.2.4 Liberdade de pensamento e expressão (art. 13) e direitos políticos (art. 23 da CADH)

Os conteúdos sintéticos agravaram o problema da desinformação: o *deepfake* simula pessoas dizendo o que jamais disseram e adultera conteúdos de forma imperceptível para o cidadão, comprometendo a participação esclarecida da qual depende a democracia (Barroso; Mello, 2024, p. 20-21), além de atingir a honra e a imagem das pessoas retratadas, com especial incidência sobre mulheres.

Para o objeto desta pesquisa, o risco relevante é duplo. De um lado, o Estado pode empregar IA para monitorar manifestações e identificar pessoas por suas posições políticas. De outro, ao enfrentar a desinformação com ferramentas automatizadas de moderação ou remoção de conteúdos, pode converter-se ele próprio em ameaça à liberdade de expressão e aos direitos políticos que pretende proteger.

Essas hipóteses afetam a liberdade de expressão e os direitos políticos. A CADH protege as dimensões individual e social da liberdade de expressão (Corte IDH, 1985, § 30-32), veda a censura prévia e as restrições indiretas (Brasil, 1992, art. 13.2 e 13.3) e assegura a participação política (Brasil, 1992, art. 23.1). Em *San Miguel Sosa y otras vs. Venezuela*, a dispensa de servidoras após a divulgação de lista de signatários de referendo revogatório levou a Corte IDH a reconhecer desvio de poder e violação dos direitos políticos e da liberdade de expressão (Corte IDH, 2018b), precedente pertinente diante da capacidade da IA de monitorar pessoas por suas posições políticas. A Relatoria Especial recomenda privilegiar medidas não restritivas contra a desinformação eleitoral (CIDH, 2019), como a rotulagem de conteúdos sintéticos adotada pelo Tribunal Superior Eleitoral (TSE) (Brasil, 2024); a remoção automatizada de conteúdos pelo Estado, ao contrário, deve observar integralmente o art. 13, sob pena de converter-se em censura.

2.2.5 Vida, integridade e liberdade pessoais (arts. 4, 5 e 7 da CADH)

Os sistemas de IA dependem de grandes volumes de dados para seu treinamento e funcionamento, o que amplia os riscos de vazamentos e de ataques cibernéticos (Barroso; Mello, 2024, p. 22). Além das vulnerabilidades comuns a qualquer sistema informatizado, a IA apresenta superfícies de ataque próprias: no serviço público, um sistema de triagem processual manipulado pode desviar casos, e uma ferramenta biométrica sujeita a ataques de evasão pode gerar falsos negativos ou falsos positivos. Braga e Perez Filho (2025, p. 23) ressaltam que a segurança cibernética e a robustez dos sistemas são vitais para protegê-los contra manipulações e falhas capazes de comprometer a integridade das decisões judiciais.

Somam-se a isso as "alucinações" da IA generativa, isto é, a produção de informações falsas com aparência de veracidade (Braga; Perez Filho, 2025, p. 6), que, inseridas em minutas ou relatórios, podem contaminar a fundamentação de atos estatais.

Quando ocorrem em infraestruturas críticas, na triagem de chamadas de emergência ou em serviços de saúde, ou quando produzem erros de identificação que conduzem a prisões, essas falhas alcançam a vida, a integridade e a liberdade pessoais (Brasil, 1992, arts. 4.1, 5.1 e 7).

Aplicam-se a esses sistemas os deveres de prevenção (Corte IDH, 1988, § 174-175) e de regular e fiscalizar serviços prestados por particulares (Corte IDH, 2006c, § 98-99), e a exigência de fatos objetivos para a detenção (Corte IDH, 2020c) impede que um alerta automatizado baste para fundamentar uma prisão. Ocorrido o dano, subsistem integralmente os deveres de investigar e reparar.

3 SISTEMAS DE INTELIGÊNCIA ARTIFICIAL DE ALTO RISCO NO EU AI ACT

O Regulamento (UE) 2024/1689 organiza seu arcabouço normativo a partir do grau de risco de cada sistema, graduando as exigências conforme o potencial de dano de cada tecnologia (Braga; Perez Filho, 2025, p. 11) e concentrando os requisitos mais rígidos nas aplicações de maior potencial de dano à saúde, à segurança e aos direitos fundamentais (Soares, 2025, p. 18). Embora tenha alcance extraterritorial (União Europeia, 2024, art. 2º, n. 1) e possa converter-se em padrão global de fato, no chamado "efeito Bruxelas" (Soares, 2025, p. 21), o regulamento não se aplica aos atos do Estado brasileiro praticados em seu território, razão pela qual é aqui utilizado apenas como referência comparativa.

Esta seção examina a categoria dos sistemas de "risco elevado" (expressão da versão oficial em língua portuguesa, aqui tratada como sinônimo de alto risco), disciplinada no Capítulo III do regulamento.

3.1 A abordagem baseada em riscos e as práticas proibidas

O regulamento estrutura-se em quatro níveis de risco. O risco mínimo, como o de filtros de *spam*, não gera obrigações vinculativas (União Europeia, 2024, art. 95). O risco limitado, próprio de *chatbots* e geradores de conteúdo sintético, impõe deveres de transparência para que as pessoas saibam que interagem com uma máquina ou que o conteúdo foi gerado artificialmente (União Europeia, 2024, art. 50). O risco elevado abrange sistemas com potencial de causar prejuízos significativos à saúde, à segurança e aos direitos fundamentais, permitidos mediante requisitos rigorosos. E o risco inaceitável corresponde a práticas incompatíveis com os valores da União e, por isso, proibidas (União Europeia, 2024, art. 5º).

Entre as práticas proibidas, interessam diretamente à atuação estatal a pontuação social de pessoas, a avaliação do risco de uma pessoa cometer infrações baseada exclusivamente na definição de perfis ou em traços de personalidade, a criação de bases de reconhecimento facial por recolha não direcionada de imagens, a categorização biométrica destinada a inferir atributos sensíveis, como raça ou opiniões políticas, e, salvo exceções taxativas, a identificação biométrica à distância em tempo real em espaços públicos para fins de aplicação da lei (União Europeia, 2024, art. 5º, n. 1, alíneas *c*, *d*, *e*, *g* e *h*). A categoria do alto risco revela, por contraste, a opção central do regulamento: não proibir determinados usos, mas condicionar sua licitude ao cumprimento de um padrão de diligência técnica e organizacional.

3.2 Critérios de classificação dos sistemas de alto risco (art. 6º e Anexo III)

O artigo 6º estabelece duas vias autônomas de qualificação de um sistema como de alto risco. A primeira alcança sistemas que sejam componentes de segurança de produtos, ou eles próprios produtos, abrangidos pela legislação de harmonização da União listada no Anexo I, como máquinas, brinquedos e dispositivos médicos, e sujeitos a avaliação de conformidade por terceiros (União Europeia, 2024, art. 6º, n. 1). A segunda, mais relevante para esta pesquisa, dispensa qualquer conexão com a segurança de produtos e qualifica como de alto risco os sistemas destinados aos usos discriminados no Anexo III (União Europeia, 2024, art. 6º, n. 2).

O Anexo III organiza esses usos em oito áreas, boa parte delas correspondente a funções tipicamente estatais, como a identificação biométrica à distância, a avaliação da elegibilidade para prestações de assistência pública, a avaliação do risco de reincidência e o apoio a autoridades judiciárias na interpretação dos fatos e do direito. A lista pode ser alterada pela Comissão Europeia, considerando, entre outros critérios, a gravidade do dano potencial e o desequilíbrio de poder entre o responsável pela utilização e a pessoa afetada (União Europeia, 2024, art. 7º).

O calendário de aplicação dessas regras foi recentemente alterado pelo *Digital Omnibus on AI* (Van Eecke; Regenhardt, 2026), publicado como Regulamento (UE) 2026/1744, que adiou as obrigações do Anexo III para 2 de dezembro de 2027 e as do Anexo I para 2 de agosto de 2028, mantido até 2 de agosto de 2030 o prazo de adequação dos sistemas de autoridades públicas já em serviço (União Europeia, 2024, art. 111, n. 2).

3.3 Obrigações e salvaguardas aplicáveis

Uma vez classificado como de alto risco, o sistema sujeita-se, ao longo de todo o seu ciclo de vida, a sete requisitos cumulativos: gestão de riscos (art. 9º), governança dos dados (art. 10), documentação técnica (art. 11), registro de eventos (art. 12), transparência (art. 13), supervisão humana (art. 14) e exatidão, robustez e cibersegurança (art. 15).

Dois desses requisitos relacionam-se diretamente com os riscos examinados na seção 2. O artigo 10 exige que os dados sejam pertinentes e suficientemente representativos e impõe o exame de enviesamentos suscetíveis de afetar direitos fundamentais ou de conduzir a discriminações, bem como a adoção de medidas para detectá-los, preveni-los e atenuá-los (União Europeia, 2024, art. 10, n. 2, alíneas *f* e *g*). O artigo 14 exige interfaces que permitam aos supervisores compreender os resultados, manter-se conscientes da tendência de confiar excessivamente na máquina (viés de automação) e desconsiderar ou reverter os resultados. Na

identificação biométrica à distância, nenhuma medida pode ser tomada com base no resultado sem verificação separada por, pelo menos, duas pessoas com competência e autoridade para tanto, regra que, todavia, pode ser afastada para fins de aplicação da lei, migração e controle de fronteiras (União Europeia, 2024, art. 14, n. 5).

Entre as obrigações dos operadores da cadeia de valor, interessam sobretudo as do responsável pela implantação, posição ocupada pelo Estado quando utiliza sistema desenvolvido por terceiro: utilizar o sistema conforme as instruções, atribuir a supervisão humana a pessoas com competência e autoridade, monitorar o funcionamento e suspender o uso diante de risco, conservar os registros e informar as pessoas afetadas de que estão sujeitas a sistema de alto risco (União Europeia, 2024, art. 26).

Duas salvaguardas adicionais merecem destaque. A primeira é a avaliação de impacto sobre os direitos fundamentais, obrigatória para implementadores que sejam organismos de direito público ou prestadores privados de serviços públicos, a ser realizada antes da primeira utilização, com descrição dos processos, das pessoas afetadas, dos riscos de danos, das medidas de supervisão humana e das providências a adotar caso os riscos se materializem (União Europeia, 2024, art. 27), modelo que Braga e Perez Filho (2025, p. 14-15) apontam como importante para o setor público brasileiro. A segunda consiste nos direitos das pessoas afetadas de apresentar reclamação à autoridade de fiscalização e de obter explicações claras e significativas sobre o papel do sistema na decisão que produza efeitos jurídicos ou as afete significativamente (União Europeia, 2024, arts. 85 e 86).

3.4 Síntese: complementaridade e distinção entre regulação técnica e proteção internacional

A correlação realizada na seção 2 demonstra que a utilização estatal de IA não é um problema apenas tecnológico, pois se traduz em interferências potenciais sobre direitos protegidos pela CADH, para as quais a jurisprudência interamericana já oferece parâmetros, ainda que formulados em termos abertos. Em relação ao regulamento europeu examinado nesta seção, a relação é de complementaridade, mas não de identidade. O EU AI Act é instrumento preventivo e de conformidade, dirigido aos operadores da cadeia de valor, ao passo que a CADH estabelece obrigações estatais cujo descumprimento é apurado em âmbito nacional e internacional e gera dever de reparação, e, em pontos como a proibição do resultado discriminatório e as garantias processuais em matéria penal, exige mais do que o regulamento. A própria Corte IDH recorre com frequência à jurisprudência da Corte Europeia de Direitos

Humanos como recurso argumentativo (Pereira, 2026), o que confirma a legitimidade do diálogo, desde que preservada a autonomia do parâmetro interamericano.

3.5 Limites do modelo europeu e cautelas na sua utilização como referência para o Brasil

A densidade do regime europeu não deve ocultar seus limites, a começar pela natureza do instrumento. O EU AI Act é, fundamentalmente, um regulamento de mercado interno e de segurança de produtos: embora declare o objetivo de proteger os direitos fundamentais (União Europeia, 2024, art. 1º, n. 1), opera por meio de requisitos e avaliações de conformidade, em regra realizadas pelo próprio fornecedor no caso dos sistemas do Anexo III, e os direitos individuais que cria restringem-se, em essência, à reclamação administrativa e à explicação da decisão.

Pesam também as exceções que alcançam justamente a atuação estatal mais sensível. O regulamento não se aplica a sistemas utilizados exclusivamente para fins militares, de defesa ou de segurança nacional (União Europeia, 2024, art. 2º, n. 3), admite exceções para fins de aplicação da lei na identificação biométrica em tempo real e na dupla verificação humana e deixa aos Estados-Membros decidir se autoridades públicas podem ser multadas (União Europeia, 2024, art. 99, n. 8).

O regulamento opera, ademais, em um ecossistema que inclui a Carta dos Direitos Fundamentais, o Regulamento Geral sobre a Proteção de Dados, a diretiva sobre o tratamento de dados para fins penais (União Europeia, 2016a; 2016b), autoridades de fiscalização dotadas de recursos e um tribunal supranacional. O Brasil, por sua vez, conta apenas com normas setoriais, como a Resolução CNJ nº 615/2025, e enfrenta desafios de capacidade técnica no modelo de governança proposto no Projeto de Lei (PL) nº 2.338/2023 (Braga; Perez Filho, 2025, p. 19). A transposição literal das obrigações europeias, sem a correspondente infraestrutura institucional, produziria apenas uma regulação simbólica.

Esses limites não afastam a utilidade do regulamento, primeira lei horizontal e abrangente sobre IA no mundo (Soares, 2025, p. 16), cujo catálogo de usos de alto risco coincide em grande medida com as funções estatais nas quais se manifestaram os riscos identificados na seção 2 e cujo modelo inspira tanto o PL nº 2.338/2023 (Soares, 2025, p. 50) quanto a classificação de riscos adotada pela Resolução CNJ nº 615/2025 (Braga; Perez Filho, 2025, p. 19). Impõem, porém, que ele seja tratado pelo que é: um repertório de soluções normativas, e não fonte de obrigação para o Estado brasileiro. O papel que pode desempenhar no controle de convencionalidade é analisado a seguir.

4 CONTROLE DE CONVENCIONALIDADE E SISTEMAS DE IA DE ALTO RISCO

4.1 Origem, fundamentos e desenvolvimento do controle de convencionalidade na Corte IDH

Moreira (2017, p. 252) conceitua o controle de convencionalidade como "a sindicância de compatibilidade vertical entre as normas estatais e o direito internacional dos direitos humanos", e seu objeto abrange atos internos comissivos ou omissivos (Ramos; Gama, 2022, p. 290). O controle é exercido em duas instâncias: na internacional, pela própria Corte IDH, ao verificar a compatibilidade de normas e práticas internas com a CADH, o que impede que os Estados sejam, ao mesmo tempo, "fiscais e fiscalizados"; e na nacional, pelos órgãos internos, no exame de compatibilidade do ordenamento interno com as normas internacionais, de caráter provisório ou preliminar em relação ao controle internacional (Ramos; Gama, 2022, p. 291).

Embora a Corte IDH já examinasse, ainda que implicitamente, a compatibilidade entre normas internas e a Convenção, exame obrigatório desde a entrada em vigor da CADH, em 1978 (Moreira, 2017, p. 255), a expressão foi consagrada, em sua dimensão interna, em *Almonacid Arellano y otros vs. Chile*, no qual a Corte IDH afirmou que o Poder Judiciário deve exercer "una especie de 'control de convencionalidad'" entre as normas internas e a CADH (Corte IDH, 2006a, § 124), e qualificada como dever de ofício, no marco das competências de cada órgão, em *Trabajadores Cesados del Congreso vs. Perú* (Corte IDH, 2006b, § 128). Em *Radilla Pacheco vs. México* e *Gelman vs. Uruguay*, a Corte acrescentou que o parâmetro inclui a interpretação que ela própria faz da Convenção (Corte IDH, 2009c, § 339; Corte IDH, 2011, § 193), inclusive no exercício de sua competência consultiva (Corte IDH, 2014c, § 31).

O fundamento normativo do instituto encontra-se nas obrigações de respeitar e garantir os direitos (art. 1.1) e de adotar disposições de direito interno (art. 2º), na regra segundo a qual nenhuma disposição da Convenção pode ser interpretada de modo a limitar direitos (art. 29) e nos princípios do direito dos tratados, especialmente o *pacta sunt servanda* e a impossibilidade de invocar o direito interno para justificar o inadimplemento de um tratado (Brasil, 2009b, arts. 26 e 27). Moreira (2017, p. 254) acrescenta a esses fundamentos o princípio da boa-fé e as cláusulas de abertura da ordem constitucional estatal, como os arts. 4º, II, e 5º, § 2º, da Constituição de 1988.

O controle de convencionalidade não transforma a Corte IDH em instância de cassação das decisões nacionais. O controle doméstico é primário, pois ao Estado "cabe a proteção primária e máxima dos direitos humanos", ao passo que o interamericano é complementar, em razão da subsidiariedade da jurisdição internacional (Moreira, 2017, p. 253). O controle orienta-

se, ademais, pela primazia da norma mais favorável à pessoa, seja ela de origem internacional ou interna, regra prevista no próprio art. 29, b, da CADH (Ramos, 2009, p. 255-256).

4.2 A extensão do controle de convencionalidade a órgãos estatais não judiciais

A jurisprudência interamericana não restringiu o controle aos juízes. Em *Cabrera García y Montiel Flores vs. México*, a Corte IDH estendeu-o aos órgãos vinculados à administração da justiça em todos os níveis (Corte IDH, 2010a, § 225). Em *Gelman vs. Uruguay*, afirmou que controlar a convencionalidade é "função e tarefa de qualquer autoridade pública e não apenas do Poder Judiciário" (Corte IDH, 2011, § 239). E, em decisões posteriores, inclusive em caso contra o Brasil, reiterou que todas as autoridades e órgãos do Estado estão obrigados a exercê-lo de ofício (Corte IDH, 2014a, § 471; 2014b, § 124; 2021a, § 204).

Essa ampliação, contudo, não foi linear. Ao examinar setenta manifestações da Corte IDH proferidas entre 2006 e 2016, Moreira (2017, p. 270) identificou quatro posicionamentos sobre quem deve exercer o controle no plano interno: os juízes e tribunais nacionais; os órgãos dotados de jurisdição; os juízes e órgãos vinculados à administração da justiça; e todos os poderes e órgãos do Estado, entendimento que, embora minoritário em termos quantitativos, tornou-se o atual. No próprio caso Gelman, a Corte afirmou, no parágrafo 193, a competência dos órgãos vinculados à administração da justiça e, no parágrafo 239, a de qualquer autoridade pública, o que leva o autor a concluir que o tribunal "vem decidindo de forma assimétrica, indo e voltando em seus entendimentos, inclusive, dentro de uma mesma decisão" (Moreira, 2017, p. 266). A crítica é pertinente no campo da IA, em que a ausência de standards interamericanos específicos poderia estimular decisões casuísticas e contraditórias.

A divergência pode ser equacionada a partir da ressalva que acompanha a própria formulação jurisprudencial: o controle é exercido no marco das competências de cada autoridade e das regulações processuais correspondentes. Propõe-se, assim, distinguir três modalidades. A primeira, exigível de todas as autoridades, consiste na interpretação do direito interno conforme a CADH e a jurisprudência interamericana. A segunda, também exigível de autoridades administrativas, consiste no dever de abster-se de praticar atos incompatíveis com a Convenção e de adotar, no exercício de suas competências, as medidas preventivas necessárias à garantia dos direitos, o que, em matéria de IA, inclui avaliar previamente os riscos de um sistema e deixar de implantá-lo quando incompatível com os direitos convencionais, em linha com o controle preventivo descrito pela doutrina (Moreira, 2017, p. 253). A terceira, consistente em

negar aplicação a lei vigente por incompatibilidade com a CADH, permanece, no desenho constitucional brasileiro, reservada aos órgãos jurisdicionais. Essa distinção, que constitui interpretação desenvolvida nesta pesquisa, aproxima-se da classificação doutrinária entre controle forte, exercido por órgãos dotados de jurisdição e apto a invalidar a norma inconvencional, e controle fraco, no qual, "em virtude da incompetência do órgão para tanto, somente poderá haver uma interpretação conforme" (Moreira, 2017, p. 253), e preserva o alcance da jurisprudência interamericana sem atribuir a autoridades administrativas competências que o ordenamento interno não lhes confere.

4.3 O controle de convencionalidade no ordenamento jurídico brasileiro

No Brasil, o controle de convencionalidade apoia-se na abertura constitucional aos tratados de direitos humanos (Brasil, 1988, art. 5º, §§ 2º e 3º) e na posição hierárquica que o Supremo Tribunal Federal (STF) lhes atribuiu. No julgamento do Recurso Extraordinário nº 466.343/SP (Brasil, 2009a), o Tribunal reconheceu que os tratados de direitos humanos não aprovados pelo rito do § 3º do art. 5º possuem status supralegal, situando-se acima da legislação ordinária e abaixo da Constituição, e consagrou o chamado "duplo estatuto" dos tratados de direitos humanos (Ramos; Gama, 2022, p. 288). Não basta, contudo, citar o texto convencional: Ramos (2009, p. 245) defende um "controle de convencionalidade aplicado", que utilize a interpretação realizada pelos órgãos internacionais instituídos pelos próprios tratados. Assim, a CADH, com status supralegal, e a Convenção Interamericana contra o Racismo, com status constitucional, funcionam como parâmetros de validade das leis e dos atos infralegais e administrativos que disciplinem ou autorizem o uso de sistemas de IA.

A recepção, contudo, não é linear. O STF declarou, por meio da Arguição de Descumprimento de Preceito Fundamental (ADPF) nº 153, compatível com a Constituição a Lei de Anistia (Brasil, 2010), cujas disposições impeditivas da investigação de graves violações a Corte IDH declarou carentes de efeitos jurídicos em *Gomes Lund y otros vs. Brasil* (Corte IDH, 2010b, § 174). Ramos e Gama (2022, p. 286) descrevem o episódio como um "choque das placas tectônicas" entre as ordens interna e internacional e propõem, para superá-lo, a teoria do duplo controle, segundo a qual qualquer ato ou norma deve ser aprovado tanto no controle de constitucionalidade quanto no de convencionalidade (Ramos; Gama, 2022, p. 292). Em *Herzog y otros vs. Brasil*, a Corte constatou que as autoridades jurisdicionais brasileiras não exerceram o controle de convencionalidade (Corte IDH, 2018a, § 292, 311 e 312) e, mais recentemente, em *Leite*,

Peres Crispim e outros vs. Brasil, de 2025, voltou a condenar o Estado por falhas na investigação e na responsabilização de graves violações (Fonsêca; Moreira, 2026, p. 10). No próprio Superior Tribunal de Justiça (STJ), a Quinta Turma afastou o crime de desacato por incompatibilidade com o art. 13 da CADH (Brasil, 2017a), entendimento superado meses depois pela Terceira Seção (Brasil, 2017b). Esses episódios revelam o potencial do instituto e sua instabilidade na prática judicial brasileira.

No plano institucional, o CNJ recomendou aos órgãos judiciais a observância dos tratados de direitos humanos e da jurisprudência da Corte IDH (CNJ, 2022), instituiu unidade de monitoramento do cumprimento de suas decisões (CNJ, 2021) e lançou o Pacto Nacional do Judiciário pelos Direitos Humanos (Ramos; Gama, 2022, p. 294-295). Em matéria de IA, a Resolução CNJ nº 615/2025, que substituiu a Resolução nº 332/2020, instituiu classificação de riscos inspirada no modelo europeu, vedou determinadas soluções e exigiu governança para as de alto risco (Braga; Perez Filho, 2025, p. 19-20; Velloso; Consalter, 2025, p. 9-12).

4.4 O controle de convencionalidade aplicado à utilização estatal de sistemas de IA de alto risco

O controle de convencionalidade não é um mecanismo abstrato de regulação tecnológica: seu objeto são as normas, os atos, as decisões e as práticas estatais que incorporam a tecnologia, já que quaisquer normas internas, inclusive leis, decretos, normas constitucionais e decisões judiciais, podem ser objeto do controle (Moreira, 2017, p. 254). Abrange os atos normativos que autorizam o uso de IA, cuja adequação o art. 2º da CADH impõe ao Poder Legislativo. Alcança também as decisões administrativas e judiciais apoiadas nesses sistemas, avaliadas segundo a motivação e a contestabilidade exigidas pelos arts. 8 e 25. Estende-se ainda às práticas administrativas, como a contratação de soluções tecnológicas e o compartilhamento de bases de dados (Brasil, 2022c), que estão sujeitas tanto ao autocontrole da Administração quanto ao controle externo; nesse plano, o controle "incide diretamente sobre a validade de atos administrativos concretos, funcionando como parâmetro de legalidade e legitimidade estatal" (Fonsêca; Moreira, 2026, p. 14).

Essa decomposição revela que a dimensão preventiva do controle cabe, sobretudo, à administração e ao legislador, destinatário, com fundamento no art. 2º da CADH, de um dever de exame preventivo de convencionalidade (Moreira, 2017, p. 262). A obrigação de garantia exige que o Estado previna razoavelmente as violações (Corte IDH, 1988, § 174-175), e, em matéria ambiental, a Corte IDH extraiu desse dever a obrigação de exigir estudos de impacto prévios a

atividades que possam causar danos significativos (Corte IDH, 2017, § 157 e 160). Sem transpor mecanicamente esse entendimento, sustenta-se, como interpretação desta pesquisa, que a implantação estatal de sistema de IA apto a afetar significativamente direitos convencionais deve ser precedida de avaliação de riscos proporcional, para a qual o art. 27 do EU AI Act oferece modelo concreto. Aos órgãos jurisdicionais cabe o controle repressivo e corretivo, sem a tarefa impossível de prevenir, sozinhos, todos os riscos da IA.

O uso do reconhecimento facial na segurança pública, prática já adotada no país e cujos efeitos desproporcionais sobre pessoas negras foram apontados na seção 2 (Oliveira, 2019; Barroso; Mello, 2024, p. 22-23), permite visualizar a aplicação desses parâmetros. O primeiro aspecto é a base legal: à luz do caso CAJAR, as faculdades estatais de vigilância e de tratamento de dados pessoais devem estar previstas em lei em sentido formal (Corte IDH, 2023, § 158), e a privação de liberdade somente pode ocorrer nas condições previamente fixadas em lei (Brasil, 1992, art. 7.2). A inexistência da legislação específica exigida pela LGPD para a segurança pública (Brasil, 2018, art. 4º, III, e § 1º) constitui, assim, indício relevante de déficit de legalidade, ou mesmo de omissão inconvencional, já que o controle alcança "não só as ações, mas também as omissões legislativas" (Moreira, 2017, p. 260), a ser enfrentado pelo Legislativo, nos termos do art. 2º da CADH, e considerado pelo Judiciário nos casos concretos.

Impõe-se, em seguida, o exame da necessidade e da proporcionalidade: se existem meios menos intrusivos, se o uso se limita a crimes graves, se há autorização prévia por autoridade independente e quais são as taxas de erro do sistema, desagregadas por raça e gênero. Como as detenções exigem fatos concretos e são arbitrárias quando fundadas em estereótipos (Corte IDH, 2020c), um alerta automatizado deve ser tratado como mero indício, a ser confirmado de forma independente por agente humano, à semelhança da dupla verificação do art. 14, n. 5, do regulamento europeu.

Exigem-se, ainda, garantias procedimentais, pois as decisões que possam afetar direitos humanos devem ser fundamentadas, sob pena de arbitrariedade (Corte IDH, 2008, § 78). Transposto para decisões apoiadas por IA, esse dever implica, como interpretação desta pesquisa, que a pessoa afetada seja informada da utilização do sistema e tenha acesso aos registros necessários para impugnar o resultado, garantias que encontram paralelo nos deveres de informação e de explicação do regulamento europeu (União Europeia, 2024, arts. 26 e 86) e no direito à revisão de decisões automatizadas (Brasil, 2018, art. 20), bem como que a decisão não se limite a reproduzir o resultado do sistema.

Constatada a incompatibilidade, as consequências podem variar da interpretação conforme e da exigência de salvaguardas adicionais à suspensão do sistema, à invalidação do ato que o autorizou e à reparação das vítimas, à semelhança da suspensão, correção ou descontinuidade prevista pela Resolução CNJ nº 615/2025 para os sistemas do Judiciário com viés discriminatório (CNJ, 2025, art. 8º, §§ 2º e 3º; Velloso; Consalter, 2025, p. 11-12).

O mesmo raciocínio alcança ferramentas semelhantes ao COMPAS eventualmente empregadas na execução penal: a administração penitenciária integra o Poder Executivo e não se submete à vedação da Resolução CNJ nº 615/2025 (CNJ, 2025, art. 10, II), lacuna que o controle de convencionalidade, fundado nos arts. 5.6, 8 e 24 da CADH, pode ajudar a suprir.

4.5 As obrigações do EU AI Act como parâmetro comparativo e elemento interpretativo

A utilidade do EU AI Act para o controle de convencionalidade decorre do fato de que as obrigações convencionais são formuladas em termos abertos: o dever de prevenir com a devida diligência não indica, por si só, quais medidas o Estado deve adotar. Nesse contexto, o regulamento pode desempenhar quatro funções: (i) referencial para identificação de riscos, pois o Anexo III e o art. 5º reúnem usos de elevado potencial de dano; (ii) indicador do padrão de diligência razoavelmente exigível, útil inclusive do ponto de vista probatório; (iii) subsídio para concretizar conceitos convencionais abertos, como necessidade, proporcionalidade e motivação; e (iv) referência para o legislador brasileiro no cumprimento do art. 2º da CADH, como já ocorre com o PL nº 2.338/2023 (Soares, 2025, p. 50). Até mesmo suas lacunas são instrutivas, pois revelam, como nas exceções para aplicação da lei e segurança nacional, os pontos em que a proteção interamericana poderá exigir mais.

O regulamento europeu, por outro lado, não é parâmetro convencional vinculante para o Brasil nem integra o bloco normativo que fundamenta o controle de convencionalidade. Não pode funcionar como teto da proteção, pois, quando a CADH ou a jurisprudência interamericana exigirem mais, prevalecem as obrigações interamericanas, por força do art. 29 da Convenção. Tampouco como piso automático, a ponto de se considerar violada a CADH pela simples ausência de uma obrigação prevista no direito europeu. Seu valor é argumentativo e comparativo, naquilo que Virgílio Afonso da Silva, citado por Pereira (2026), denomina migração de ideias constitucionais, em contraposição à transposição de regras ou de textos. Não por acaso, no próprio continente europeu, a dimensão de direitos humanos da matéria foi objeto

de tratado específico, a Convenção-Quadro do Conselho da Europa sobre Inteligência Artificial e Direitos Humanos, Democracia e Estado de Direito (Conselho da Europa, 2024).

4.6 Limites institucionais, normativos e práticos da abordagem

A abordagem proposta enfrenta limites que não podem ser ignorados. O primeiro é a opacidade: sistemas de aprendizado profundo podem ser de difícil explicação, e a invocação de segredo comercial restringe o acesso a informações essenciais para a impugnação de decisões (Sauthier, 2026, p. 10). O segundo é probatório: a vítima de discriminação algorítmica raramente dispõe dos dados necessários para demonstrar o impacto desproporcional do sistema, o que recomenda a distribuição dinâmica do ônus da prova e o acesso aos registros e à documentação técnica.

O terceiro limite refere-se à atribuição de responsabilidades: no plano internacional, a utilização de sistema desenvolvido por particular não exime o Estado, mas, no plano interno, a distribuição de deveres entre fornecedor, órgão contratante e agente público ainda carece de disciplina legal (Braga; Perez Filho, 2025, p. 23). O quarto é a capacidade técnica das instituições: sem formação adequada de magistrados e servidores, a supervisão humana corre o risco de se converter em mera formalidade (Braga; Perez Filho, 2025, p. 20-21).

O quinto limite decorre da natureza casuística e posterior do controle judicial, que contrasta com o caráter sistêmico e escalável dos danos algorítmicos (Cavalcante, 2023, p. 75): quando uma decisão reconhece a incompatibilidade de um sistema, milhares de pessoas podem já ter sido afetadas. O sexto é a ausência de *standards* interamericanos específicos sobre IA, que aumenta o risco de decisões divergentes, agravado pelas oscilações da própria Corte IDH quanto aos sujeitos do controle (Moreira, 2017, p. 270) e pela aplicação ainda desigual dos parâmetros interamericanos pelo Judiciário brasileiro (Fonsêca; Moreira, 2026, p. 6).

5 CONSIDERAÇÕES FINAIS

Verificou-se que o Brasil, ao ratificar a CADH e reconhecer a jurisdição da Corte IDH, vinculou-se ao SIDH, e que os riscos da IA estatal assumem dimensão jurídica própria em razão do poder de império, da assimetria entre autoridade e indivíduo e da vinculação direta do Estado às obrigações de respeito e garantia. Esses riscos atingem direitos que encontram proteção vinculante no SIDH, cuja jurisprudência, embora não tenha enfrentado diretamente sistemas de IA, oferece parâmetros aplicáveis, como a exigência de lei em sentido formal para a vigilância

estatal, a necessidade e a proporcionalidade das ingerências, a proibição de detenções fundadas em estereótipos, o dever de motivação e o dever de prevenção com a devida diligência. O EU AI Act, por sua vez, converte esses riscos em obrigações preventivas, mas tem natureza predominantemente regulatória e de mercado, comporta exceções justamente na atuação estatal mais sensível e teve parte de sua aplicação adiada.

À luz desses resultados, a hipótese foi confirmada com ressalvas. O controle de convencionalidade constitui parâmetro juridicamente consistente para avaliar e limitar a utilização estatal de sistemas de IA de alto risco, porque as obrigações convencionais incidem sobre toda conduta estatal, independentemente da tecnologia empregada, e porque a CADH ocupa, no Brasil, posição supralegal que lhe permite servir de parâmetro de validade para normas, atos e decisões. Sua eficácia, porém, depende de três condições: que seja exercido por todas as autoridades no marco de suas competências, com destaque para a atuação preventiva da administração, e não apenas pela magistratura; que disponha de critérios concretos para traduzir *standards* abertos em exigências verificáveis, tarefa para a qual o EU AI Act oferece contribuição relevante, como referência comparativa e elemento interpretativo, sem constituir obrigação convencional; e que existam condições institucionais mínimas de transparência, acesso a informações, capacidade técnica e responsabilização.

Como perspectiva, a construção de *standards* interamericanos sobre IA poderia ser favorecida por manifestação da Corte IDH em sede consultiva ou contenciosa. No plano interno, o art. 2º da CADH recomenda a aprovação de marco legal de IA que contemple avaliação de impacto e direitos das pessoas afetadas, a edição da legislação sobre tratamento de dados na segurança pública e na persecução penal e a extensão, aos demais Poderes, de salvaguardas semelhantes às já adotadas pelo CNJ. Enquanto essas medidas não se concretizam, o controle de convencionalidade permanece como parâmetro jurídico disponível para assegurar que a inovação tecnológica estatal não se realize à margem dos direitos humanos.

REFERÊNCIAS

BARROSO, Luís Roberto; MELLO, Patrícia Perrone Campos. Inteligência artificial: promessas, riscos e regulação: algo de novo debaixo do sol. **Revista Direito e Práxis**, Rio de Janeiro, v. 15, n. 4, p. 1-45, 2024. Disponível em: ttps://doi.org/10.1590/2179-8966/2024/84479. Acesso em: 23 out. 2026.

BRAGA, Pedro Alonso das Neves; PEREZ FILHO, Augusto Martinez. Regulamentação da inteligência artificial no Poder Judiciário: perspectivas, desafios e o diálogo entre o marco

europeu e as iniciativas brasileiras. **Revista Contemporânea**, [*S. l.*], v. 5, n. 7, p. 1-29, 2025. Disponível em: https://doi.org/10.56083/RCV5N7-035. Acesso em: 27 out. 2026.

BRASIL. Constituição (1988). **Constituição da República Federativa do Brasil**. Brasília, DF: Senado Federal, 1988. Disponível em: https://planalto.gov.br/ccivil_03/constituicao/Constituicao.htm. Acesso em: 27 out. 2026.

BRASIL. **Decreto nº 678, de 6 de novembro de 1992**. Promulga a Convenção Americana sobre Direitos Humanos (Pacto de São José da Costa Rica), de 22 de novembro de 1969. Brasília, DF: Presidência da República, 1992. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto/d0678.htm. Acesso em: 23 out. 2026.

BRASIL. **Decreto nº 1.973, de 1º de agosto de 1996**. Promulga a Convenção Interamericana para Prevenir, Punir e Erradicar a Violência contra a Mulher, concluída em Belém do Pará, em 9 de junho de 1994. Brasília, DF: Presidência da República, 1996.

BRASIL. **Decreto nº 4.463, de 8 de novembro de 2002**. Promulga a Declaração de Reconhecimento da Competência Obrigatória da Corte Interamericana de Direitos Humanos, sob reserva de reciprocidade, em consonância com o art. 62 da Convenção Americana sobre Direitos Humanos (Pacto de São José), de 22 de novembro de 1969. Brasília, DF: Presidência da República, 2002. Disponível em: https://www2.camara.leg.br/legin/fed/decret/2002/decreto-4463-8-novembro-2002-485986-publicacaooriginal-1-pe.html. Acesso em: 27 out. 2026.

BRASIL. Supremo Tribunal Federal (Tribunal Pleno). **Recurso Extraordinário 466.343/SP**. Prisão civil. Depositário infiel. Alienação fiduciária. Status supralegal dos tratados internacionais de direitos humanos. Relator: Min. Cezar Peluso, 3 de dezembro de 2008. Diário da Justiça Eletrônico, Brasília, DF, 5 jun. 2009a.

BRASIL. **Decreto nº 7.030, de 14 de dezembro de 2009**. Promulga a Convenção de Viena sobre o Direito dos Tratados, concluída em 23 de maio de 1969, com reserva aos artigos 25 e 66. Brasília, DF: Presidência da República, 2009b.

BRASIL. Supremo Tribunal Federal (Tribunal Pleno). **Arguição de Descumprimento de Preceito Fundamental 153/DF**. Lei n. 6.683/1979 (Lei de Anistia). Relator: Min. Eros Grau, 29 de abril de 2010. Diário da Justiça Eletrônico, Brasília, DF, 6 ago. 2010.

BRASIL. Superior Tribunal de Justiça (5. Turma). **Recurso Especial 1.640.084/SP**. Crime de desacato. Incompatibilidade com o art. 13 da Convenção Americana sobre Direitos Humanos. Controle de convencionalidade. Relator: Min. Ribeiro Dantas, 15 de dezembro de 2016. Diário da Justiça Eletrônico, Brasília, DF, 1 fev. 2017a.

BRASIL. Superior Tribunal de Justiça (3. Seção). **Habeas Corpus 379.269/MS**. Crime de desacato. Tipicidade. Relator para o acórdão: Min. Antonio Saldanha Palheiro, 24 de maio de 2017. Diário da Justiça Eletrônico, Brasília, DF, 30 jun. 2017b.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 23 out. 2026.

BRASIL. Supremo Tribunal Federal (Tribunal Pleno). **Referendo na Medida Cautelar na Ação Direta de Inconstitucionalidade 6.387/DF**. Medida Provisória n. 954/2020. Compartilhamento de dados de usuários de serviços de telecomunicações com o IBGE. Relatora: Min. Rosa Weber, 7 de maio de 2020. Diário da Justiça Eletrônico, Brasília, DF, 12 nov. 2020.

BRASIL. **Decreto nº 10.932, de 10 de janeiro de 2022**. Promulga a Convenção Interamericana contra o Racismo, a Discriminação Racial e Formas Correlatas de Intolerância, firmado pela República Federativa do Brasil, na Guatemala, em 5 de junho de 2013. Brasília, DF: Presidência da República, 2022a.

BRASIL. **Emenda Constitucional nº 115, de 10 de fevereiro de 2022**. Altera a Constituição Federal para incluir a proteção de dados pessoais entre os direitos e garantias fundamentais e para fixar a competência privativa da União para legislar sobre proteção e tratamento de dados pessoais. Brasília, DF: Presidência da República, 2022b. Disponível em: https://planalto.gov.br/ccivil_03/constituicao/Emendas/Emc/emc115.htm. Acesso em: 27 out. 2026.

BRASIL. Supremo Tribunal Federal (Tribunal Pleno). **Ação Direta de Inconstitucionalidade 6.649/DF e Arguição de Descumprimento de Preceito Fundamental 695/DF**. Compartilhamento de dados pessoais no âmbito da administração pública federal. Decreto n. 10.046/2019. Relator: Min. Gilmar Mendes, 15 de setembro de 2022. Brasília, DF: STF, 2022c.

BRASIL. Senado Federal. **Projeto de Lei nº 2.338, de 2023**. Dispõe sobre o desenvolvimento, o fomento e o uso ético e responsável da inteligência artificial com base na centralidade da pessoa humana. Brasília, DF: Senado Federal, 2023. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2487262. Acesso em: 23 out. 2026.

BRASIL. Tribunal Superior Eleitoral. **Resolução nº 23.732, de 27 de fevereiro de 2024**. Altera a Res.-TSE nº 23.610, de 18 de dezembro de 2019, que dispõe sobre a propaganda eleitoral. Brasília, DF: TSE, 2024. Disponível em: https://www.tse.jus.br/legislacao/compilada/res/2024/resolucao-no-23-732-de-27-de-fevereiro-de-2024. Acesso em: 27 out. 2026.

CAVALCANTE, Jamile Sabbad Carecho. **Os desafios éticos no desenvolvimento de sistemas inteligentes no Poder Judiciário brasileiro**: uma perspectiva acerca dos riscos aos direitos fundamentais. 2023. 191 f. Dissertação (Mestrado em Direito) – Universidade Estácio de Sá, Rio de Janeiro, 2023.

COMISSÃO INTERAMERICANA DE DIREITOS HUMANOS (CIDH). Relatoría Especial para la Libertad de Expresión. **Libertad de expresión e Internet**. Washington, D.C.: OEA, 2013. (OEA/Ser.L/V/II. CIDH/RELE/INF. 11/13).

COMISSÃO INTERAMERICANA DE DIREITOS HUMANOS (CIDH). Relatoría Especial para la Libertad de Expresión. **Estándares para una Internet libre, abierta e incluyente**. Washington, D.C.: OEA, 2017. (OEA/Ser.L/V/II. CIDH/RELE/INF.17/17).

COMISSÃO INTERAMERICANA DE DIREITOS HUMANOS (CIDH). Relatoría Especial para la Libertad de Expresión. **Guía para garantizar la libertad de expresión frente a la desinformación deliberada en contextos electorales**. Washington, D.C.: OEA, 2019.

CONSELHO DA EUROPA. **Convenção-Quadro do Conselho da Europa sobre Inteligência Artificial e Direitos Humanos, Democracia e Estado de Direito**. Vilnius, 5 set. 2024. (Council of Europe Treaty Series, n. 225).

CONSELHO NACIONAL DE JUSTIÇA (CNJ). **Resolução nº 364, de 12 de janeiro de 2021**. Dispõe sobre a instituição da Unidade de Monitoramento e Fiscalização de decisões e deliberações da Corte Interamericana de Direitos Humanos no âmbito do Conselho Nacional de Justiça. Brasília, DF: CNJ, 2021.

CONSELHO NACIONAL DE JUSTIÇA (CNJ). **Recomendação nº 123, de 7 de janeiro de 2022**. Recomenda aos órgãos do Poder Judiciário brasileiro a observância dos tratados e convenções internacionais de direitos humanos e o uso da jurisprudência da Corte Interamericana de Direitos Humanos. Brasília, DF: CNJ, 2022.

CONSELHO NACIONAL DE JUSTIÇA (CNJ). **Resolução nº 615, de 11 de março de 2025**. Estabelece diretrizes para o desenvolvimento, utilização e governança de soluções desenvolvidas com recursos de inteligência artificial no Poder Judiciário. Brasília, DF: CNJ, 2025.

CORTE INTERAMERICANA DE DIREITOS HUMANOS (Corte IDH). **Opinión Consultiva OC-5/85, de 13 de noviembre de 1985**. La colegiación obligatoria de periodistas (arts. 13 y 29 Convención Americana sobre Derechos Humanos). San José: Corte IDH, 1985. (Serie A, n. 5).

CORTE INTERAMERICANA DE DIREITOS HUMANOS (Corte IDH). **Caso Velásquez Rodríguez vs. Honduras**. Fondo. Sentencia de 29 de julio de 1988. San José: Corte IDH, 1988. (Serie C, n. 4).

CORTE INTERAMERICANA DE DIREITOS HUMANOS (Corte IDH). **Opinión Consultiva OC-16/99, de 1 de octubre de 1999**. El derecho a la información sobre la asistencia consular en el marco de las garantías del debido proceso legal. San José: Corte IDH, 1999. (Serie A, n. 16).

CORTE INTERAMERICANA DE DIREITOS HUMANOS (Corte IDH). **Caso del Tribunal Constitucional vs. Perú**. Fondo, reparaciones y costas. Sentencia de 31 de enero de 2001. San José: Corte IDH, 2001. (Serie C, n. 71).

CORTE INTERAMERICANA DE DIREITOS HUMANOS (Corte IDH). **Opinión Consultiva OC-18/03, de 17 de septiembre de 2003**. Condición jurídica y derechos de los migrantes indocumentados. San José: Corte IDH, 2003. (Serie A, n. 18).

CORTE INTERAMERICANA DE DIREITOS HUMANOS (Corte IDH). **Caso Almonacid Arellano y otros vs. Chile**. Excepciones preliminares, fondo, reparaciones y costas. Sentencia de 26 de septiembre de 2006. San José: Corte IDH, 2006a. (Serie C, n. 154).

CORTE INTERAMERICANA DE DIREITOS HUMANOS (Corte IDH). **Caso Trabajadores Cesados del Congreso (Aguado Alfaro y otros) vs. Perú**. Excepciones preliminares, fondo, reparaciones y costas. Sentencia de 24 de noviembre de 2006. San José: Corte IDH, 2006b. (Serie C, n. 158).

CORTE INTERAMERICANA DE DIREITOS HUMANOS (Corte IDH). **Caso Ximenes Lopes vs. Brasil**. Sentencia de 4 de julio de 2006. San José: Corte IDH, 2006c. (Serie C, n. 149).

CORTE INTERAMERICANA DE DIREITOS HUMANOS (Corte IDH). **Caso Apitz Barbera y otros ("Corte Primera de lo Contencioso Administrativo") vs. Venezuela**. Excepción preliminar, fondo, reparaciones y costas. Sentencia de 5 de agosto de 2008. San José: Corte IDH, 2008. (Serie C, n. 182).

CORTE INTERAMERICANA DE DIREITOS HUMANOS (Corte IDH). **Caso Escher y otros vs. Brasil**. Excepciones preliminares, fondo, reparaciones y costas. Sentencia de 6 de julio de 2009. San José: Corte IDH, 2009a. (Serie C, n. 200).

CORTE INTERAMERICANA DE DIREITOS HUMANOS (Corte IDH). **Caso González y otras ("Campo Algodonero") vs. México**. Excepción preliminar, fondo, reparaciones y costas. Sentencia de 16 de noviembre de 2009. San José: Corte IDH, 2009b. (Serie C, n. 205).

CORTE INTERAMERICANA DE DIREITOS HUMANOS (Corte IDH). **Caso Radilla Pacheco vs. Estados Unidos Mexicanos**. Excepciones preliminares, fondo, reparaciones y costas. Sentencia de 23 de noviembre de 2009. San José: Corte IDH, 2009c. (Serie C, n. 209).

CORTE INTERAMERICANA DE DIREITOS HUMANOS (Corte IDH). **Caso Cabrera García y Montiel Flores vs. México**. Excepción preliminar, fondo, reparaciones y costas. Sentencia de 26 de noviembre de 2010. San José: Corte IDH, 2010a. (Serie C, n. 220).

CORTE INTERAMERICANA DE DIREITOS HUMANOS (Corte IDH). **Caso Gomes Lund y otros ("Guerrilha do Araguaia") vs. Brasil**. Excepciones preliminares, fondo, reparaciones y costas. Sentencia de 24 de noviembre de 2010. San José: Corte IDH, 2010b. (Serie C, n. 219).

CORTE INTERAMERICANA DE DIREITOS HUMANOS (Corte IDH). **Caso Gelman vs. Uruguay**. Fondo y reparaciones. Sentencia de 24 de febrero de 2011. San José: Corte IDH, 2011. (Serie C, n. 221).

CORTE INTERAMERICANA DE DIREITOS HUMANOS (Corte IDH). **Caso Atala Riffo y niñas vs. Chile**. Fondo, reparaciones y costas. Sentencia de 24 de febrero de 2012. San José: Corte IDH, 2012. (Serie C, n. 239).

CORTE INTERAMERICANA DE DIREITOS HUMANOS (Corte IDH). **Caso de Personas Dominicanas y Haitianas Expulsadas vs. República Dominicana**. Excepciones preliminares, fondo, reparaciones y costas. Sentencia de 28 de agosto de 2014. San José: Corte IDH, 2014a. (Serie C, n. 282).

CORTE INTERAMERICANA DE DIREITOS HUMANOS (Corte IDH). **Caso Liakat Ali Alibux vs. Suriname**. Excepciones preliminares, fondo, reparaciones y costas. Sentencia de 30 de enero de 2014. San José: Corte IDH, 2014b. (Serie C, n. 276).

CORTE INTERAMERICANA DE DIREITOS HUMANOS (Corte IDH). **Opinión Consultiva OC-21/14, de 19 de agosto de 2014**. Derechos y garantías de niñas y niños en el contexto de la migración y/o en necesidad de protección internacional. San José: Corte IDH, 2014c. (Serie A, n. 21).

CORTE INTERAMERICANA DE DIREITOS HUMANOS (Corte IDH). **Caso Velásquez Paiz y otros vs. Guatemala**. Excepciones preliminares, fondo, reparaciones y costas. Sentencia de 19 de noviembre de 2015. San José: Corte IDH, 2015. (Serie C, n. 307).

CORTE INTERAMERICANA DE DIREITOS HUMANOS (Corte IDH). **Opinión Consultiva OC-23/17, de 15 de noviembre de 2017**. Medio ambiente y derechos humanos. San José: Corte IDH, 2017. (Serie A, n. 23).

CORTE INTERAMERICANA DE DIREITOS HUMANOS (Corte IDH). **Caso Herzog y otros vs. Brasil**. Excepciones preliminares, fondo, reparaciones y costas. Sentencia de 15 de marzo de 2018. San José: Corte IDH, 2018a. (Serie C, n. 353).

CORTE INTERAMERICANA DE DIREITOS HUMANOS (Corte IDH). **Caso San Miguel Sosa y otras vs. Venezuela**. Fondo, reparaciones y costas. Sentencia de 8 de febrero de 2018. San José: Corte IDH, 2018b. (Serie C, n. 348).

CORTE INTERAMERICANA DE DIREITOS HUMANOS (Corte IDH). **Caso Azul Rojas Marín y otra vs. Perú**. Excepciones preliminares, fondo, reparaciones y costas. Sentencia de 12 de marzo de 2020. San José: Corte IDH, 2020a. (Serie C, n. 402).

CORTE INTERAMERICANA DE DIREITOS HUMANOS (Corte IDH). **Caso Empleados de la Fábrica de Fuegos en Santo Antônio de Jesus y sus familiares vs. Brasil**. Excepciones preliminares, fondo, reparaciones y costas. Sentencia de 15 de julio de 2020. San José: Corte IDH, 2020b. (Serie C, n. 407).

CORTE INTERAMERICANA DE DIREITOS HUMANOS (Corte IDH). **Caso Fernández Prieto y Tumbeiro vs. Argentina**. Fondo y reparaciones. Sentencia de 1 de septiembre de 2020. San José: Corte IDH, 2020c. (Serie C, n. 411).

CORTE INTERAMERICANA DE DIREITOS HUMANOS (Corte IDH). **Caso Barbosa de Souza y otros vs. Brasil**. Excepciones preliminares, fondo, reparaciones y costas. Sentencia de 7 de septiembre de 2021. San José: Corte IDH, 2021a. (Serie C, n. 435).

CORTE INTERAMERICANA DE DIREITOS HUMANOS (Corte IDH). **Caso de los Buzos Miskitos (Lemoth Morris y otros) vs. Honduras**. Sentencia de 31 de agosto de 2021. San José: Corte IDH, 2021b. (Serie C, n. 432).

CORTE INTERAMERICANA DE DIREITOS HUMANOS (Corte IDH). **Caso Miembros de la Corporación Colectivo de Abogados "José Alvear Restrepo" vs. Colombia**. Excepciones preliminares, fondo, reparaciones y costas. Sentencia de 18 de octubre de 2023. San José: Corte IDH, 2023. (Serie C, n. 506).

CRESTANE, Dérique Soares. **Discriminação algorítmica**: a aplicabilidade dos standards protetivos fixados pela Corte Interamericana de Direitos Humanos e pelo Supremo Tribunal Federal em relação ao direito de igualdade e não discriminação a partir das noções de ius

constitutionale commune latino-americano e dever de proteção estatal. 2023. 182 f. Dissertação (Mestrado em Direito) – Universidade de Santa Cruz do Sul, Santa Cruz do Sul, 2023.

FONSÊCA, Marina Soares da; MOREIRA, Thiago Oliveira. O controle de convencionalidade no Judiciário brasileiro: a atuação do Tribunal Regional Federal da 5ª Região em caso de revisão de anistia política. **Revista da Faculdade de Direito de São Bernardo do Campo**, São Bernardo do Campo, v. 32, n. 1, 2026.

MOREIRA, Thiago Oliveira. O exercício do controle de convencionalidade pela Corte Interamericana de Direitos Humanos: uma década de decisões assimétricas. *In*: MENEZES, Wagner (org.). **Direito internacional em expansão**. Belo Horizonte: Arraes, 2017. v. 10, p. 251-271.

NAÇÕES UNIDAS; ORGANIZAÇÃO PARA A SEGURANÇA E COOPERAÇÃO NA EUROPA; ORGANIZAÇÃO DOS ESTADOS AMERICANOS; COMISSÃO AFRICANA DOS DIREITOS HUMANOS E DOS POVOS. **Joint declaration on artificial intelligence and freedom of expression**. [*S. l.*], 24 out. 2025. Disponível em: https://teaching.globalfreedomofexpression.columbia.edu/node/756. Acesso em: 23 out. 2026.

OLIVEIRA, Caroline. Cerca de 90% das pessoas presas com uso de reconhecimento facial são negras. **Brasil de Fato**, São Paulo, 27 nov. 2019. Disponível em: https://www.brasildefato.com.br/2019/11/27/cerca-de-90-das-pessoas-presas-com-uso-de-reconhecimento-facial-sao-negras. Acesso em: 23 out. 2026.

ORGANIZAÇÃO DOS ESTADOS AMERICANOS (OEA). Comitê Jurídico Interamericano. **Principios actualizados del Comité Jurídico Interamericano sobre la privacidad y la protección de datos personales**. Washington, D.C.: OEA, 2021.

PEREIRA, Claudio José Langroiva. Teoria da convencionalidade. *In*: PEREIRA, Claudio José Langroiva. **Processo penal e convencionalidade**. Rio de Janeiro: Almedina Brasil, 2026. cap. 3. E-book.

RAMOS, André de Carvalho. Supremo Tribunal Federal brasileiro e o controle de convencionalidade: levando a sério os tratados de direitos humanos. **Revista da Faculdade de Direito da Universidade de São Paulo**, São Paulo, v. 104, p. 241-286, jan./dez. 2009.

RAMOS, André de Carvalho; GAMA, Marina Faraco Lacerda. Controle de convencionalidade, teoria do duplo controle e o Pacto Nacional do Judiciário pelos Direitos Humanos: avanços e desafios. **Revista Direitos Culturais**, Santo Ângelo, v. 17, n. 41, p. 283-297, jan./abr. 2022. DOI: 10.20912/rdc.v17i41.756.

REIS, Graziela Tavares de Souza. Inteligência artificial e direito internacional: gênero, algoritmos e decolonialidade. *In:* MENEZES, Wagner (org.). **Direito internacional em expansão**. [*S. l.*]: [*s. n.*], 2026. v. 29, p. 537-554.

SAUTHIER, Priscila. Discriminação algorítmica e a dignidade humana: o impacto ao respeito, à autonomia e à autodeterminação. **Revista Algoritmos & Sociedade**, Belo Horizonte, v. 1, n. 1, p. 1-21, 2026. Disponível em: https://periodicos.ufmg.br/index.php/algoritmosesociedade/article/view/61140. Acesso em: 27 out. 2026.

SOARES, Vítor Fonseca. **Panorama mundial da legislação de inteligência artificial**. Brasília, DF: Câmara dos Deputados, Consultoria Legislativa, 2025. Estudo técnico. Disponível em: https://www2.camara.leg.br/a-camara/estruturaadm/secretarias/secretaria-da-inovacao-legislativa/publicacoes/panorama-mundial-da-legislacao-de-inteligencia-artificial/view. Acesso em: 27 out. 2026.

UNIÃO EUROPEIA. Diretiva (UE) 2016/680 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, deteção ou repressão de infrações penais ou execução de sanções penais, e à livre circulação desses dados. **Jornal Oficial da União Europeia**, Luxemburgo, L 119, p. 89-131, 4 maio 2016a.

UNIÃO EUROPEIA. Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados). **Jornal Oficial da União Europeia**, Luxemburgo, L 119, p. 1-88, 4 maio 2016b.

UNIÃO EUROPEIA. Regulamento (UE) 2024/1689 do Parlamento Europeu e do Conselho, de 13 de junho de 2024, que cria regras harmonizadas em matéria de inteligência artificial (Regulamento da Inteligência Artificial). **Jornal Oficial da União Europeia**, Luxemburgo, Série L, 12 jul. 2024. Disponível em: https://eur-lex.europa.eu/eli/reg/2024/1689/oj/por. Acesso em: 27 out. 2026.

VAN EECKE, Patrick; REGENHARDT, Bartholomäus. Digital AI Omnibus delays key deadlines, introduces new rules. **Cooley**: cyber/data/privacy insights, [*S. l.*], 3 ago. 2026. Disponível em: https://cdp.cooley.com/digital-ai-omnibus-delays-key-deadlines-introduces-new-rules/. Acesso em: 23 out. 2026.

VELLOSO, Larissa Cimarelli; CONSALTER, Zilda Mara. Políticas anti viés algorítmico no Poder Judiciário brasileiro: um estudo crítico da Resolução CNJ nº 615/2020 [*sic*]. **Revista Brasileira de Direito e Justiça**, Ponta Grossa, v. 9, p. 1-19, e2525463, 2025. Disponível em: https://doi.org/10.5212/RBDJ.v.9.25463.003. Acesso em: 27 out. 2026.