ReGeo ISSN: 2177-3246

DADOS BIOMÉTRICOS: UMA ANÁLISE DO PROJETO DE LEI 2338/2023 A PARTIR DOS PARÂMETROS ESTABELECIDOS NO AI ACT DA UNIÃO EUROPEIA

BIOMETRIC DATA: AN ANALYSIS OF BILL 2338/2023 BASED ON THE PARAMETERS ESTABLISHED IN THE EUROPEAN UNION AI ACT

DATOS BIOMÉTRICOS: UN ANÁLISIS DEL PROYECTO DE LEY 2338/2023 A PARTIR DE LOS PARÁMETROS ESTABLECIDOS EN EL AI ACT DE LA UNIÓN EUROPEA

10.56238/revgeov17n1-087

Joaquim Ribeiro de Souza Junior
Doutorando em Direito e Mestre em Direito
Instituição: Pontifícia Universidade Católica do Rio Grande do Sul (PUCRS)
E-mail: joaquimjunior33@gmail.com
Orcid: https://orcid.org/0000-0003-3488-5508

Glenda Almeida Matos Moreira
Doutoranda em Direito e Mestre em Sociologia
Instituição: Pontifícia Universidade Católica do Rio Grande do Sul (PUCRS) e Centro Universitário
E-mail: glendaalmeidamoreira@gmail.com
Orcid: https://orcid.org/0000-0002-8940-3644

RESUMO
O artigo examina o tratamento jurídico dos dados e sistemas biométricos no Projeto de Lei nº 2.338/2023 (marco brasileiro de inteligência artificial) à luz dos parâmetros do Regulamento (UE) 2024/1689 (AI Act). Parte-se da constatação de que a biometria, embora enquadrada como dado pessoal sensível pela LGPD, vem sendo amplamente utilizada no Brasil em serviços públicos e privados, especialmente em infraestrutura estatal de identificação (por exemplo, bancos civis e sistemas como AFIS/ABIS) e em aplicações de reconhecimento facial em espaços públicos, cenário que tem gerado controvérsias por erros, vieses e impactos discriminatórios. A pesquisa, de caráter qualitativo e documental, descreve conceitos operacionais (identificação biométrica, verificação/autenticação, identificação biométrica remota, reconhecimento de emoções e categorização biométrica), apresenta as principais escolhas regulatórias do AI Act (regulação por risco, práticas proibidas, requisitos para sistemas de alto risco e salvaguardas para identificação biométrica remota em tempo real) e, em seguida, analisa o PL 2338/2023, com foco na vedação, como regra, da identificação biométrica à distância em tempo real em espaços acessíveis ao público, nas hipóteses de exceção e nas obrigações de governança, transparência e avaliação de impacto algorítmico para usos no setor público. O cotejo revela convergência estrutural entre os modelos (proibição com exceções tipificadas e regime reforçado para alto risco), mas também aponta lacunas e oportunidades de aprimoramento no projeto brasileiro: detalhamento de salvaguardas e supervisão externa para exceções, trilhas de auditoria e deveres claros de descarte; proibição expressa de formação/expansão de bases faciais por raspagem não direcionada; disciplina mais densa para identificação biométrica remota "posterior" (ex post); e limites específicos para categorização biométrica e para reconhecimento de emoções em contextos assimétricos, como trabalho e educação. Conclui-se que os

parâmetros europeus oferecem referências concretas para fortalecer a proteção de direitos fundamentais e a responsabilização no uso de biometria mediado por IA no Brasil.

Palavras-chave: Dados Biométricos. Identificação Biométrica Remota. Reconhecimento Facial. PL 2338/2023. AI Act. Regulação por Risco.

ABSTRACT
This article analyzes how biometric data and biometric systems are regulated in Brazil's Bill of Law No. 2,338/2023 (the proposed Brazilian AI framework) in light of the standards set by Regulation (EU) 2024/1689 (the AI Act). It starts from the premise that biometrics, although classified as sensitive personal data under the LGPD, has expanded rapidly in Brazil across public and private settings, notably through state identification infrastructures and facial recognition deployments in publicly accessible spaces. Such uses have fueled controversy due to error rates, bias, and discriminatory impacts. Using a qualitative, documentary approach, the study outlines core operational concepts (biometric identification, verification/authentication, remote biometric identification, emotion recognition, and biometric categorization), summarizes the AI Act's risk-based architecture (prohibited practices, high-risk requirements, and safeguards for real-time remote biometric identification), and then examines the bill's main biometric provisions. The comparison shows a shared regulatory backbone: a general ban on real-time remote biometric identification in publicly accessible spaces with narrowly defined exceptions, coupled with stronger governance, transparency, and impact-assessment duties for high-risk uses. At the same time, the article identifies gaps and improvement paths for the Brazilian bill inspired by the AI Act, including: more granular procedural safeguards and independent oversight for exceptions; audit trails and clear deletion duties; an explicit prohibition on building or expanding facial databases through untargeted scraping; a clearer framework for 'post' remote biometric identification (ex post searches); and more specific limits on biometric categorization and emotion recognition in asymmetric environments such as workplaces and educational institutions. The article concludes that the EU framework offers actionable parameters to strengthen fundamental-rights protection and accountability in biometric AI deployments in Brazil.

Keywords: Biometric Data. Remote Biometric Identification. Facial Recognition. Bill 2,338/2023. EU AI Act. Risk-Based Regulation.

RESUMEN
El artículo analiza el tratamiento normativo de los datos y sistemas biométricos en el Proyecto de Ley nº 2.338/2023 (marco brasileño de inteligencia artificial) a partir de los parámetros del Reglamento (UE) 2024/1689 (AI Act). Se parte de que la biometría, aunque es dato personal sensible en la LGPD, se ha expandido en Brasil en ámbitos públicos y privados, en especial en infraestructuras estatales de identificación y en el reconocimiento facial en espacios de acceso público, con controversias por errores, sesgos e impactos discriminatorios. Con metodología cualitativa y documental, el estudio delimita conceptos operativos (identificación biométrica, verificación/autenticación, identificación biométrica remota, reconocimiento de emociones y categorización biométrica), sintetiza el enfoque de regulación por riesgo del AI Act (prácticas prohibidas, obligaciones para sistemas de alto riesgo y salvaguardas para la identificación remota en tiempo real) y contrasta esas categorías con la disciplina propuesta en el PL 2.338/2023. La comparación muestra convergencias: prohibición general de la identificación biométrica remota en tiempo real en espacios accesibles al público con excepciones tipificadas y deberes reforzados de gobernanza y transparencia. Asimismo, identifica mejoras posibles inspiradas en el AI Act: mayor detalle de salvaguardas y supervisión independiente para las excepciones (trazabilidad y deberes de eliminación), prohibición expresa del raspado no dirigido para crear o ampliar bases faciales, tratamiento claro de la identificación remota "posterior" (ex post) y límites específicos para categorización biométrica y reconocimiento de emociones en contextos asimétricos como trabajo y educación.

Palabras clave: Datos Biométricos. Identificación Biométrica Remota. Reconocimiento Facial. PL 2338/2023. Ley de IA. Regulación por Riesgo.

1 INTRODUÇÃO

A expansão do uso de dados biométricos e de sistemas biométricos no Brasil aparece em registros institucionais e na literatura como fenômeno associado à identificação e verificação de identidade em contextos públicos e privados, com aplicações em segurança pública, controle de acesso a serviços e transações digitais.

Essa dinâmica insere a biometria em arranjos técnicos que dependem de coleta, armazenamento e comparação automatizada de características físicas, fisiológicas ou comportamentais, o que amplia o papel de infraestruturas de dados e de mecanismos decisórios baseados em modelos computacionais.

No campo jurídico brasileiro, dados biométricos figuram como dados pessoais sensíveis na Lei Geral de Proteção de Dados (LGPD), o que condiciona seu tratamento a hipóteses legais específicas e a deveres de observância de princípios como finalidade, necessidade e transparência.

Entretanto, nesse contexto há controvérsias públicas sobre usos de vigilância biométrica e com registros de erros, vieses e contestação social, em especial em aplicações de reconhecimento facial em espaços públicos e em práticas privadas de exposição de imagens de suspeitos.

Recentemente, a União Europeia aprovou o Regulamento (UE) 2024/1689, conhecido como AI Act, que estrutura um regime de regulação por risco para sistemas de inteligência artificial e inclui disciplina específica para usos biométricos, com proibições, categorias operacionais e requisitos procedimentais, especialmente para identificação biométrica remota em tempo real em espaços publicamente acessíveis.

Já no Brasil, a discussão sobre um marco de inteligência artificial se consolidou no Projeto de Lei nº 2338/2023 (PL 2338), que propõe regime de classificação de risco, deveres de governança e instrumentos como avaliação de impacto algorítmico, além de trazer definições operacionais de identificação biométrica e autenticação biométrica e disciplina específica para identificação biométrica à distância em tempo real em espaços acessíveis ao público, com regra de vedação e hipóteses de exceção.

Este artigo analisa o tratamento normativo da biometria no PL nº 2338/2023 a partir dos parâmetros do AI Act, com foco em identificação biométrica remota, autenticação, reconhecimento de emoções e outros usos biométricos que envolvem vigilância, categorização e tomada de decisão mediada por sistemas de IA. A investigação adota abordagem qualitativa e documental, com exame comparado de dispositivos do PL e do AI Act, além de leitura de materiais institucionais e de literatura utilizada para contextualizar usos e controvérsia.

A partir desse recorte, o texto busca identificar convergências e lacunas regulatórias na disciplina de biometria, com especial atenção a salvaguardas procedimentais, deveres de transparência e mecanismos de responsabilização associados ao uso de sistemas biométricos em contextos públicos e privados.

A estrutura do artigo parte de uma contextualização conceitual sobre biometria e sistemas biométricos e de seus usos no Brasil, incluindo parâmetros normativos nacionais e controvérsias recentes, e em seguida descreve os elementos centrais do AI Act sobre biometria. Na sequência, examina o PL nº 2338/2023 com foco em seus dispositivos biométricos e realiza a comparação entre os regimes, para formular síntese das convergências e das perspectivas normativas que emergem do cotejo entre as duas matrizes regulatórias e, então, demonstrar as perspectivas do AI Act para o direito brasileiro.

2 BIOMETRIA E INTELIGÊNCIA ARTIFICIAL

No contexto da identificação humana, a biometria pode ser compreendida como um conjunto de técnicas que estabelece a identidade de uma pessoa a partir de atributos físicos e comportamentais, com emprego de métodos estatísticos, biológicos e tecnológicos e com base na captura de dados pessoais.

Os dados biométricos, por sua vez, são os dados pessoais resultantes de tratamento técnico específico relativo a características físicas, fisiológicas ou comportamentais, capazes de permitir ou confirmar a identificação única do titular, com exemplos como imagens faciais e dados dactiloscópicos, que pode servir a autenticação, identificação ou classificação de pessoas, com emprego tanto por empresas quanto por governos (Silva, 2023).

Nesse sentido, parte da literatura diferencia biometria como campo técnico e dado biométrico como produto de um processamento técnico sobre uma característica, o que aproxima o debate de governança de dados, pois o traço corporal passa a circular como informação operacionalizável por máquinas e por terceiros (Silva, 2023).

Ressalta-se, também, as definições adotadas pelo Brasil (2019). O Decreto 10.046/2019 diferencia dados biográficos — aqueles relativos a fatos da vida da pessoa, como nome civil ou social, data de nascimento, filiação, naturalidade, nacionalidade, sexo, estado civil, grupo familiar, endereço e vínculos empregatícios —, e dados biométricos, características biológicas e comportamentais mensuráveis, coletáveis para reconhecimento automatizado, como palma da mão, digitais, retina ou íris, formato da face, voz e maneira de andar.

Segundo Violato et. al (2013), sistemas biométricos operam a partir dessas características para reconhecimento automatizado. Estes costumam empregar sensores para capturar a característica, produzir um modelo biométrico e armazená-lo em base de dados, o que viabiliza comparações futuras para identificar ou verificar indivíduos em situações concretas. Sistemas de reconhecimento biométrico tendem a incluir etapa de treinamento com amostras reais, em que a qualidade e a representatividade da base de treinamento se associam ao desempenho do sistema na população alvo.

Essa área, recentemente, foi incrementada com a Inteligência Artificial, possibilitando, assim, a extensão e a eficiência desses sistemas. O reconhecimento facial, por exemplo, é aplicação de inteligência artificial que se utiliza de coleta biométrica baseada em traços do rosto. Esse processo ocorre por medição de pontos da face e por extração de um dado biométrico que viabiliza verificação e autenticação, com transformação dessas medidas em representação numérica e armazenamento frequente para comparações futuras (Baccarin, 2023).

Como destaca Silva (2023), a captura costuma ocorrer por câmeras digitais integradas a software com algoritmos de inteligência artificial que analisam a imagem, medem características e produzem um modelo biométrico armazenado para retroalimentação do sistema, o que pode ocorrer em tempo real e em escala ampliada conforme o arranjo técnico implantado.

Assim, em termos de resultado, há descrição de que o reconhecimento facial opera por semelhança e por juízo de probabilidade, o que significa que a saída do sistema não corresponde a resposta certa, mas a correspondência mais provável dentro do conjunto comparado, com ocorrência de falso negativo e falso positivo influenciados por fatores como fundo e iluminação.

O uso de reconhecimento facial pode também se articular a práticas de perfilamento, com criação de perfis digitais a partir de informações coletadas e com possibilidade de categorização por atributos, o que amplia a circulação do dado biométrico para além do ato inicial de autenticação (Doneda, 2006 apud Silva, 2023).

2.1 PARÂMETROS NORMATIVOS BRASILEIROS SOBRE O USO DE BIOMETRIA

No Brasil, dados biométricos integram a categoria de dados pessoais sensíveis, o que submete seu tratamento a requisitos específicos e a hipóteses legais próprias (ANPD, 2025). A ANPD registra que a LGPD não definiu dados biométricos, e que parte da doutrina utiliza a descrição do GDPR, na qual dados biométricos resultam de tratamento técnico relativo a características físicas, fisiológicas ou comportamentais que permitem ou confirmam identificação única.

O tratamento de dados biométricos, enquanto sensíveis, deve se apoiar nas hipóteses do art. 11 da LGPD, com previsão de consentimento específico e destacado, ou de bases sem consentimento vinculadas a finalidades delimitadas, como obrigação legal, políticas públicas, estudos, exercício de direitos, proteção da vida, tutela da saúde e prevenção à fraude e segurança do titular em processos de identificação e autenticação em sistemas eletrônicos (Baccarin, 2023).

No mesmo recorte, há registro de que dados sensíveis não podem ser tratados com base em legítimo interesse ou proteção do crédito, o que restringe alternativas frequentemente utilizadas para dados não sensíveis.

Em aplicações privadas e público delegadas, parte da literatura enfatiza a alínea “g” do art. 11, que admite o tratamento para prevenção à fraude e segurança do titular em processos de identificação

e autenticação de cadastro em sistemas eletrônicos, com ressalva expressa quanto à prevalência de direitos e liberdades fundamentais do titular e com exigências de informação sobre finalidades e tempo de armazenamento (Silva, 2023).

A operacionalização dessas bases legais se articula aos princípios da LGPD, com destaque para finalidade, necessidade e transparência, inclusive na avaliação de alternativas menos intrusivas e na documentação de processos de tratamento em sistemas biométricos (Baccarin, 2023). Há também referência a deveres de transparência e à vinculação do tratamento à finalidade informada ao titular, com vedação de usos posteriores incompatíveis, além da enunciação de direitos do titular como confirmação de tratamento, acesso, correção e pedidos relacionados a anonimização, bloqueio ou eliminação conforme o caso (Brasil, 2018).

A LGPD prevê deveres de segurança da informação ao longo do ciclo de tratamento, inclusive após o término, e admite a exigência de relatório de impacto à proteção de dados pessoais, inclusive sensíveis, com descrição de dados coletados, metodologia e medidas de mitigação de riscos. Esse ponto aparece como parâmetro de governança para operações que dependem de bases biométricas e de sistemas automatizados de comparação, dado o potencial de impacto decorrente de erros e de usos incompatíveis com a finalidade declarada (ANPD, 2025).

No âmbito da administração pública federal, o já mencionado Decreto 10.046/2019 estabelece normas e diretrizes para compartilhamento de dados entre órgãos e entidades, institui o Cadastro Base do Cidadão e define atributos biográficos e biométricos, com biometria entendida como características biológicas e comportamentais mensuráveis coletáveis para reconhecimento automatizado (Brasil, 2019). O decreto também delimita seu escopo ao indicar que suas regras não se aplicam ao compartilhamento com o setor privado, o que mantém a LGPD como eixo central para operações empresariais e para cooperações específicas fora do arranjo.

No Cadastro Base do Cidadão, há vedação ao uso do cadastro ou de seu cruzamento com outras bases para tratamentos destinados a mapear ou explorar comportamentos individuais ou coletivos sem consentimento expresso, prévio e específico, e sem transparência da motivação e finalidade.

Além disso, a ANPD registra que, além das previsões dos arts. 5 e 11 da LGPD, pode endereçar biometria por documentos orientativos e por regulamentação, com diretrizes sobre conceitos, contextos legítimos, hipóteses legais, observância de princípios e medidas de proteção adotadas por agentes de tratamento (ANPD, 2025). Ainda, mesmo quando o tratamento ocorre sob exceções legais associadas a segurança pública, defesa nacional ou persecução penal, princípios e direitos de proteção de dados devem ser observados.

2.2 OS PROEMINENTES USOS DE DADOS E SISTEMAS BIOMÉTRICOS NO BRASIL

A biometria, no contexto das tecnologias da informação, tem como objetivos a identificação e o mapeamento de indivíduos, com justificação em segurança no acesso a bens e serviços e em segurança pública interna e de fronteiras, em articulação com expansão de bases e usos no setor público e no setor privado (Corrêa e Loureiro, 2023).

No Brasil, por exemplo, há registro institucional de ampliação do tratamento de dados biométricos. Esse conjunto de usos, se relaciona a infraestruturas estatais de identificação e verificação biométrica (ANPD, 2025), principalmente nas áreas de segurança pública e na persecução penal.

Veja-se que a constituição de bancos biométricos por órgãos públicos decorre de exigências normativas associadas à expedição de documento de identidade, passaporte, acesso a plataformas de serviços públicos e emissão ou renovação do título de eleitor, situações em que a identificação do solicitante inclui a coleta de dados biométricos. Esses dados, em especial impressões digitais, permanecem armazenados após a entrega do serviço, com possibilidade de verificação posterior conforme o contexto de coleta, o que caracteriza a formação de bancos biométricos civis no setor público (Lima et al., 2022).

Assim, é de se mencionar, por exemplo, a celebração de acordos de cooperação para permitir o acesso, por órgãos de polícia judiciária, a bancos biométricos civis como padrão para processos de identificação criminal, em cenário no qual se aponta a inexistência de legislação específica sobre produção de prova pericial com base em padrões biométricos de origem civil (Lima et al., 2022)

Nessa infraestrutura, o Automated Fingerprint Identification System, conhecido como AFIS, utiliza impressões digitais para identificar indivíduos e busca impedir duplicações de identificação ou múltiplas identificações atribuídas a uma mesma pessoa. O Manual de Identificação de Vítimas de Desastres da Polícia Federal, inclusive, recomenda o uso do sistema e indica, como medida inicial para obtenção de dados ante mortem, a inserção de fichas decadactilares para confrontos automatizados com material papiloscópico questionado (Polícia Federal, 2011 apud Souza et al., 2023).

Também se observa a adoção de sistemas multimodais, como o Automated Biometric Identification System, conhecido como ABIS, que admite reconhecimento facial, impressões palmares e impressões digitais, com apresentação de classificação por score como medida do nível de coincidência entre amostra e padrões armazenados (Souza et al., 2023). A Secretaria de Defesa Social de Pernambuco adquiriu o sistema em 2019, e a alimentação do banco de dados tem sido feita por novas emissões de carteiras de identidade e pela digitalização gradual de prontuários físicos (BGSDS, 2019 apud Souza et al., 2023).

Mais recentemente, o Programa Smart Sampa, iniciativa sob responsabilidade da Secretaria Municipal de Segurança Urbana de São Paulo, tem a previsão de instalação de 20 mil câmeras na cidade, orientada por critérios territoriais associados a índices de criminalidade, e com emprego de

algoritmos que geram alertas para intrusão, vandalismo e furtos, além de identificação de placas de veículos furtados ou roubados e reconhecimento facial voltado à localização de pessoas desaparecidas e foragidos da justiça (Prefeitura de São Paulo, 2025).

No relatório institucional de transparência do programa, o reconhecimento facial aparece associado à identificação de procurados e foragidos da Justiça e à localização de pessoas desaparecidas, com indicação de que o programa não estrutura banco de dados próprio e não armazena dados pessoais, exceto imagens vinculadas a um identificador referente a procurado, foragido ou desaparecido, e com descrição de que o acesso a informações constantes no BNMP ocorre quando há compatibilidade facial superior a 90 por cento.

No setor privado, a biometria aparece principalmente como técnica de autenticação e identificação em atividades cotidianas, com deslocamento parcial de métodos tradicionais como senhas e cartões para credenciais baseadas em características biológicas do titular (Canuto, 2022). Esse movimento também se associa à lógica de segurança no acesso a bens e serviços no mercado e à difusão de tecnologias de identificação biométrica em conexão com tecnologias da informação (Correa e Loureiro, 2023).

Segundo Canuto (2022), os dados biométricos utilizados por empresas podem derivar de modalidades diversas, como assinatura, impressões digitais e face, além de íris, retina, voz, geometria da mão e outras técnicas, o que amplia o debate para além do reconhecimento facial. Em termos de aplicações, há menção a cenários como controle de acesso lógico e físico e detecção de fraudes, com emprego de características como face, impressão digital e voz, entre outras.

No setor privado, a centralidade de bases de dados biométricos também intensifica discussões sobre segurança e legalidade do uso, pois o comprometimento desses dados se associa à irrevogabilidade de características do titular, o que diferencia o cenário de incidentes envolvendo senhas e justifica a adoção de técnicas específicas de proteção, como biometria cancelável e criptografia.

2.3 CONTROVÉRSIAS E RISCOS ASSOCIADOS À UTILIZAÇÃO DA BIOMETRIA

Não há unanimidade quanto ao interesse público na utilização desses sistemas, tanto na esfera pública quanto privada. Por exemplo, a Campanha Tire Meu Rosto da Sua Mira mobiliza sociedade civil no Brasil para pressionar por banimento total do reconhecimento facial digital na segurança pública, com atuação por meio de diálogo direto com forças de segurança e parlamentares, divulgação de cartas abertas e ações de educação pública sobre danos associados ao reconhecimento facial, com menção ao risco de perpetuação de racismo (EPIC, 2024).

Da mesma forma, há registro de movimentos de organizações civis que demandam regulamentação do reconhecimento facial e, em alguns casos, defendem banimento parcial ou

completo, com indicação de apoio de entidades como LAPIN, Artigo 19, Data Privacy Brasil, InternetLab e Idec à campanha Tire Meu Rosto da Sua Mira (Baccarin, 2023).

Na fundamentação pública dessas iniciativas, são apresentados exemplos associados a falsos alertas e a abordagens derivadas de sistemas de reconhecimento facial, com alegação de incidência seletiva sobre pessoas negras. Entre os casos citados, consta episódio de abril de 2025 no qual um idoso de 80 anos foi confundido com pessoa procurada pela Justiça e permaneceu detido por 10 horas após alerta atribuído a câmeras do Smart Sampa em uma unidade básica de saúde, além dos relatos de uma mulher em Sergipe confundida duas vezes em 2024 e de uma servidora pública abordada e conduzida à delegacia no Rio de Janeiro em razão de erro do sistema (Coalizão Direitos na Rede, 2025).

Paralelamente, o recente caso envolvendo a Havan S.A., rede varejista, ilustra os riscos associados. Em 2024, a empresa passou a publicar, em redes sociais, vídeos sob a denominação "amostradinhos do mês", com exposição de imagens de pessoas apontadas como autoras de furtos nas lojas, acompanhada de justificativa empresarial de inibição da prática por meio da exposição pública (Gercina, 2024).

O sistema de monitoramento utilizava inteligência artificial que, segundo declaração pública atribuída à direção da empresa, permite identificar pessoas ao entrar ou sair da loja e relacionar o registro facial ao momento do furto, o que indica uso de técnicas automatizadas de identificação a partir de imagens capturadas no estabelecimento.

Em maio de 2025, a ANPD recebeu notificação do Ministério Público do Estado de Santa Catarina com solicitação de análise de compatibilidade da prática com a LGPD, fato que inseriu a conduta em procedimento de fiscalização da autoridade. Após análise preliminar, a Coordenação-Geral de Fiscalização determinou, no final de junho de 2025, medida preventiva para suspender temporariamente a divulgação dos vídeos nas redes sociais durante a apuração, com indicação expressa de fundamentos na LGPD, em especial os artigos 6º, 7º, 11, 14 e 55-J, e com identificação de risco associado à eventual exposição de imagens de crianças e adolescentes sem cautelas exigidas pela legislação (ANPD, 2025).

Diante desse cenário, que certamente se repete com suas próprias particularidades em outros países, é necessário que se construa um arcabouço normativo específico para tratar sobre o processamento de dados biométricos por Inteligência Artificial.

3 AI ACT E O USO DE BIOMETRIA

O Regulamento (UE) 2024/1689 surge em contexto no qual sistemas de IA circulam entre Estados Membros e podem ser implantados em setores variados, com risco de fragmentação regulatória

quando normas nacionais divergem e reduzem a segurança jurídica de agentes econômicos que desenvolvem, importam ou utilizam esses sistemas (Parlamento Europeu e Conselho, 2024).

Nesse enquadramento, o regulamento vincula sua justificativa à melhoria do funcionamento do mercado interno, por meio de um quadro jurídico uniforme para desenvolvimento, colocação no mercado, entrada em serviço e uso de sistemas de IA na União, com preservação da livre circulação de bens e serviços baseados em IA e prevenção de restrições nacionais não previstas no próprio ato.

Quanto à sua finalidade, o texto preambular explicita a promoção de uma adoção de IA centrada no ser humano e compatível com valores da União, ao mesmo tempo em que prevê proteção de saúde, segurança e direitos fundamentais previstos na Carta, incluindo democracia, Estado de Direito e proteção ambiental, além de medidas de apoio à inovação.

O Artigo 1 estabelece um conjunto de eixos normativos que inclui regras harmonizadas para colocação no mercado, entrada em serviço e uso de sistemas de IA, proibições de determinadas práticas, requisitos específicos e obrigações para sistemas de alto risco e seus operadores, regras de transparência para certos sistemas, disciplina para modelos de IA de finalidade geral, além de regras de monitoramento, fiscalização, governança e medidas de apoio à inovação com foco em pequenas e médias empresas e startups.

O regulamento se destina a uma cadeia de agentes. O Artigo 2 inclui provedores[1] que colocam no mercado ou colocam em serviço sistemas de IA e provedores de modelos de IA de finalidade geral, mesmo quando estabelecidos fora da União, além de implantadores estabelecidos na União, importadores e distribuidores, fabricantes que colocam um sistema de IA no mercado sob seu nome ou marca, representantes autorizados de provedores não estabelecidos na União, e pessoas afetadas localizadas na União, quando a saída do sistema é utilizada no território europeu. O texto exclui do seu âmbito áreas fora do alcance do direito da União e declara que não afeta competências dos Estados Membros em matéria de segurança nacional, além de afastar sua aplicação a sistemas de IA usados exclusivamente para fins militares, de defesa ou de segurança nacional.

A arquitetura regulatória opera por classificação de risco e por obrigações proporcionais, com referência na literatura a quatro categorias, proibido, alto risco, risco limitado e risco mínimo, o que organiza a incidência de proibições, requisitos e deveres ao longo do ciclo de vida de sistemas e modelos (Arantes Júnior, 2025). Essa estrutura convive com a regra de que o regulamento atua de forma complementar a outros ramos do direito da União, inclusive proteção de dados, defesa do consumidor, direitos fundamentais, emprego e segurança de produtos, sem afastar direitos e meios de tutela previstos nesses regimes.

[1] No Regulamento (UE) 2024/1689, provedor é a pessoa natural ou jurídica, autoridade pública, agência ou outro organismo que desenvolve um sistema de IA ou um modelo de IA de finalidade geral, ou que manda desenvolver esse sistema ou modelo e o coloca no mercado ou o coloca em serviço sob seu próprio nome ou marca, com ou sem pagamento (Parlamento Europeu e Conselho, 2024).

O Regulamento (UE) 2024/1689 adota definições de biometria alinhadas ao vocabulário do Regulamento (UE) 2016/679, ao tratar dado biométrico como dado pessoal resultante de tratamento técnico específico relativo a características físicas, fisiológicas ou comportamentais da pessoa natural, com exemplo de imagens faciais e dados datiloscópicos (Parlamento Europeu e Conselho, 2024). No General Protection Data Regulation (GPDR), essa noção inclui o requisito de permitir ou confirmar a identificação única da pessoa, também com menção a imagens faciais e dados datiloscópicos (Parlamento Europeu e Conselho, 2016).

Essa coordenação conceitual importa porque o GDPR enquadra como categoria especial o tratamento de dados biométricos para fins de identificação única e estabelece, como regra, a proibição desse tratamento, ressalvadas hipóteses previstas no próprio Artigo 9. O AI Act incorpora essa lógica ao estabelecer que, fora do recorte específico de uso para fins de repressão penal em espaços publicamente acessíveis, o tratamento biométrico continua sujeito às exigências do GDPR e, para fins não relacionados a segurança pública, o Artigo 9 do GDPR opera como norma de proibição com exceções limitadas.

O AI Act opera por uma dinâmica regulatória baseada em risco, com diferenciação de obrigações conforme a categoria do sistema, lógica também descrita na literatura como estrutura que segmenta sistemas proibidos, de alto risco e de risco mínimo ou baixo (Monteiro, 2026).

Assim, quando se fala em biometria, o regulamento define categorias operacionais para delimitar obrigações e vedações. Identificação biométrica (*Biometric identification*) refere-se ao reconhecimento automatizado para estabelecer identidade por comparação com base de referência, enquanto verificação biométrica (*biometric verification*) designa verificação um para um, inclusive autenticação.

O texto também diferencia *remote biometric identification*, que identifica pessoas sem participação ativa, tipicamente à distância, por comparação com base de referência, e explicita a modalidade *real-time* quando captura, comparação e identificação ocorrem instantaneamente, ou quase.

Sistema de reconhecimento de emoções *(Emotion recognition system)* é definido como sistema que infere emoções ou intenções a partir de dados biométricos, e *biometric categorisation system* como sistema que atribui categorias com base em biometria, ressalvada a hipótese de função acessória e necessária por razões técnicas objetivas.

O Artigo 5 do AI Act lista práticas proibidas, com incidência direta sobre biometria. Entre elas, inclui-se a criação ou expansão de bases de reconhecimento facial por raspagem não direcionada de imagens faciais na internet ou em CCTV[2].

[2] CCTV é a sigla de *closed circuit television*, em português "circuito fechado de televisão". Refere-se a sistemas de câmeras que capturam e transmitem imagens para um conjunto restrito de monitores, gravadores ou centrais de monitoramento, em

O regulamento também veda sistemas de categorização que, com base em dados biométricos, deduzem ou inferem raça, opiniões políticas, filiação sindical, crenças religiosas ou filosóficas, vida sexual ou orientação sexual, com ressalvas delimitadas para rotulagem ou filtragem de conjuntos de dados biométricos adquiridos licitamente e para categorizações no contexto de segurança pública.

Quanto ao uso de identificação biométrica remota em tempo real em espaços publicamente acessíveis para fins de segurança pública, o AI Act estabelece proibição com exceções tipificadas e condicionadas. É dizer, o texto admite o uso apenas quando estritamente necessário para busca direcionada de vítimas específicas e pessoas desaparecidas, prevenção de ameaça substancial e iminente à vida ou segurança física ou ameaça terrorista, ou localização e identificação de suspeito por delitos graves definidos por referência a anexo e limiar de pena máxima.

Para a implementação dessas exceções, o regulamento há a previsão de salvaguardas, com exigência de avaliação de impacto sobre direitos fundamentais e registro do sistema, admitida exceção por urgência para o registro, sem afastar sua posterior conclusão.

O AI Act associa biometria a casos de alto risco, com justificativa normativa vinculada a efeitos discriminatórios e vieses, especialmente em identificação biométrica remota, razão pela qual deve ser tratada de acordo com essa particularidade. Para sistemas de alto risco, o regulamento impõe um sistema de gerenciamento de risco ao longo do ciclo de vida, definido como processo contínuo e iterativo com identificação de riscos conhecidos e previsíveis, avaliação de riscos sob uso normal e mau uso previsível, e adoção de medidas direcionadas de mitigação.

O texto estabelece ainda dever de testes para identificar medidas de gestão de riscos, com execução antes da colocação no mercado ou entrada em serviço, com métricas e limiares probabilísticos compatíveis com a finalidade pretendida.

Na dimensão de dados, exige-se que conjuntos de treinamento, validação e teste sejam submetidos a práticas de governança e gestão adequadas ao propósito, abrangendo origem dos dados e finalidade original, operações de preparação como rotulagem e limpeza, formulação de pressupostos, e exame de vieses com potencial de afetar direitos fundamentais ou conduzir a discriminação proibida no direito da União, com medidas para detectar, prevenir e mitigar.

Da mesma forma, no plano organizacional, o regulamento estabelece que provedores de sistemas de alto risco mantenham sistema de gestão da qualidade com políticas e procedimentos documentados, incluindo estratégias de conformidade, procedimentos de teste e validação e sistemas de gestão de dados.

Essas exigências estão diretamente relacionadas ao impacto sobre direitos fundamentais. Por essa razão, prevê também a avaliação desses impactos anteriormente à utilização do sistema

vez de transmitir publicamente. Em contextos urbanos e privados, CCTV costuma designar redes de videomonitoramento usadas para segurança, controle de acesso e registro de ocorrências.

biométrico, devendo conter descrição do processo em que o sistema será usado, período e frequência de uso, categorias potencialmente afetadas, riscos de danos e medidas de supervisão humana, entre outros elementos. Essa obrigação é requisito ex ante para sistemas de risco elevado na União Europeia, com possibilidade de atualização quando informações se tornarem obsoletas (Monteiro, 2026).

4 ANÁLISE DO PL 2338/2023 SOB A PERSPECTIVA DA UTILIZAÇÃO DE BIOMETRIA

A atual discussão normativa sobre inteligência artificial no Brasil ocorre em cenário no qual já existem normas que tangenciam sistemas automatizados, como a Lei Geral de Proteção de Dados e a Lei do Governo Digital, sem que haja, até o momento, um marco normativo específico e abrangente voltado exclusivamente à regulação de IA. Nesse quadro, o tema passou a integrar a agenda legislativa sob argumento de necessidade de acompanhar avanços tecnológicos e de enfrentar riscos relacionados à privacidade, à segurança, à transparência e à proteção de direitos fundamentais, com convergência do debate no PL 2.338/2023 (Arantes Júnior, 2025).

O projeto se apresenta como proposta de marco legal para regular uso, implementação e desenvolvimento de sistemas de IA no país, com previsão de mecanismos associados a avaliações de impacto e a estruturas de governança articuladas à proteção de dados pessoais (Monteiro, 2026).

No mesmo sentido, o projeto adota lógica de regulação por risco, com definição de categorias e com imposição de obrigações mais densas para sistemas classificados como de alto risco, incluindo previsões de avaliação de impacto, mecanismos de transparência e possibilidade de auditoria e supervisão por autoridades competentes (Arantes Júnior, 2025).

A tramitação do PL 2.338/2023 se conecta a iniciativas anteriores que buscaram disciplinar o uso de sistemas de IA no Brasil, com destaque para o PL 21/2020, que propôs princípios, direitos e deveres, e que foi declarado prejudicado em dezembro de 2024 em razão da tramitação posterior de propostas mais abrangentes no Senado. Além disso, outros projetos correlatos foram apensados ou considerados prejudicados, sob justificativa de evitar sobreposição normativa e concentrar o debate em torno de um marco regulatório único.

Nesse contexto, o PL 2.338/2023, de autoria do Senador Rodrigo Pacheco, foi aprovado pelo Senado Federal e remetido à Câmara dos Deputados em março de 2025. O PL 2.338/2023 organiza obrigações a partir de um modelo de classificação de risco e prevê que sistemas reputados como de alto risco, após avaliação preliminar, se submetem à avaliação de impacto algorítmico, definida como processo iterativo contínuo ao longo do ciclo de vida, com atualizações periódicas cuja periodicidade depende de regulamentação da autoridade competente, além de previsão de realização por profissionais com independência funcional e conhecimentos técnicos, científicos e jurídicos.

Na caracterização doutrinária, essa engenharia busca antecipar potenciais danos associados ao funcionamento dos sistemas, com registro de riscos conhecidos e previsíveis e de consequências adversas, em paralelo a mecanismos voltados à transparência e à responsabilização (Monteiro, 2026).

4.1 ORGANIZAÇÃO DO PROJETO DE LEI E DISPOSIÇÕES SOBRE BIOMETRIA

O texto aprovado na Câmara introduz definições operacionais para diferenciar identificação biométrica e autenticação biométrica. A identificação biométrica aparece como método que envolve o reconhecimento de características físicas, fisiológicas e comportamentais humanas com o propósito de identificar um indivíduo, enquanto a autenticação biométrica se associa ao processo de verificação ou confirmação de identidade por meio de comparação das características biométricas com um modelo previamente armazenado (Brasil, 2023). Assim, cria uma base conceitual para separar usos voltados à atribuição de identidade em um conjunto aberto de pessoas, no caso da identificação, de usos voltados à confirmação de uma identidade previamente declarada, no caso da autenticação.

No regime de classificação de risco, o PL prevê vedações específicas relacionadas à biometria em espaços acessíveis ao público. O art. 13, inciso IV, veda o desenvolvimento, a implementação e o uso de sistemas de identificação biométrica à distância em tempo real em espaços acessíveis ao público, admitindo exceções vinculadas a hipóteses delimitadas, como instrução de inquérito ou processo criminal mediante autorização judicial prévia e motivada e outros contextos enumerados no dispositivo (Brasil, 2023).

Além das vedações, o PL enquadra determinados usos biométricos como de alto risco. Entre as hipóteses listadas, consta o emprego de sistemas de identificação e autenticação biométrica para reconhecimento de emoções, com ressalva para sistemas de autenticação biométrica cujo único objetivo seja a confirmação de uma pessoa singular específica. Essa opção normativa delimita um recorte no qual o risco não decorre apenas do emprego de biometria, mas do objetivo inferencial associado ao sistema, no caso, inferências sobre estados afetivos (Brasil, 2023).

No âmbito de governança e obrigações procedimentais, o PL trata diretamente de sistemas biométricos para fins de identificação no setor público. O art. 23, § 1º, estabelece que a utilização de sistemas biométricos para fins de identificação deve observar os princípios e medidas de governança da lei e deve ser precedida de avaliação de impacto algorítmico, com observância de garantias para o exercício de direitos de pessoas ou grupos afetados e proteção contra discriminação direta, indireta, ilegal ou abusiva.

Assim, o §2º prevê que, se não houver eliminação ou mitigação substantiva dos riscos identificados, a utilização será descontinuada

Na tramitação na Câmara, uma controvérsia aparece em torno de tecnologias de reconhecimento facial em espaços públicos, em especial quando associadas à segurança pública e à

persecução penal. Documento de organizações da sociedade civil registra oposição à proposta atribuída ao relator Aguinaldo Ribeiro de afrouxar regras de uso de reconhecimento facial em espaços públicos e menciona declaração na qual o texto aprovado pelos senadores foi descrito como restritivo demais (Coalizão Direitos na Rede, 2025).

No mesmo documento, aponta-se que a redação do PL classifica tecnologias de reconhecimento facial como de risco excessivo, mas com rol amplo de exceções que abarca usos correntes no contexto de segurança pública e persecução penal, com referência ao art. 13, inciso VII, e com crítica a um cenário no qual exceções ficariam fora da estrutura de governança proposta

4.2 CONVERGÊNCIAS E NOVAS PERSPECTIVAS ENTRE O PL 2338/2023 E O AI ACT DA UNIÃO EUROPEIA

Ambos os textos normativos adotam lógica de escalonamento por risco, com um conjunto de vedações para usos considerados incompatíveis com direitos e liberdades e um regime de obrigações reforçadas para usos classificados como de alto risco. No AI Act, o art. 5 reúne práticas proibidas, inclusive por razões associadas a vigilância e a impactos sobre direitos fundamentais, e estabelece exceções delimitadas para identificação biométrica remota em tempo real em espaços publicamente acessíveis para fins de aplicação da lei, vinculadas a objetivos específicos e a um recorte de crimes referidos em anexo (União Europeia, 2024).

Já no PL 2338/2023, o art. 13 veda, como regra, o uso de sistemas de identificação biométrica à distância em tempo real em espaços acessíveis ao público, com hipóteses de exceção associadas a investigação e persecução penal, busca de vítimas e desaparecidos, ameaça grave e iminente, flagrante e cumprimento de mandados, sob requisitos como autorização judicial prévia e controle judicial quando cabível (Brasil, 2023).

Também há convergência na previsão de medidas de governança e documentação para usos de alto risco. O PL exige, no setor público, protocolos de acesso e uso com registro de quem utilizou o sistema, direito à explicação e revisão humanas e publicização de avaliações preliminares, além de impor avaliação de impacto algorítmico para uso de biometria com finalidade de identificação e descontinuidade do uso quando não houver eliminação ou mitigação substantiva de riscos.

No AI Act, a disciplina de alto risco se conecta a mecanismos de avaliação, registro e supervisão, inclusive com exigências que relacionam registro em base europeia e síntese de avaliação de impacto em direitos fundamentais em certos contextos de registro e reporte.

Por fim, nesse quadro, a principal implicação comparativa para o Brasil, com foco exclusivo em biometria, reside menos na reafirmação do núcleo já previsto no art. 13, inciso IV, e mais na possibilidade de ampliar a disciplina para outros usos biométricos com potencial de identificação e de vigilância.

5 CONSIDERAÇÕES FINAIS

Como visto, Projeto de Lei nº 2338/2023 já incorpora disciplina direta para a identificação biométrica à distância em tempo real em espaços acessíveis ao público, ao vedar o desenvolvimento, a implementação e o uso dessa prática, com exceções delimitadas, como instrução de inquérito ou processo criminal mediante autorização judicial prévia e motivada, busca de vítimas e pessoas desaparecidas, ameaça grave e iminente, flagrante delito e recaptura e cumprimento de mandados, além de exigir proporcionalidade e estrita necessidade, controle judicial e revisão da inferência algorítmica por agente público, com remissão aos princípios e direitos da própria lei e, no que couber, da LGPD (Brasil, 2023).

O AI Act estrutura solução semelhante ao tratar a identificação biométrica remota em tempo real em espaços publicamente acessíveis para finalidades de atividades de autoridades de aplicação da lei, com um regime que parte de proibição e admite uso apenas quando estritamente necessário para objetivos taxativos, como busca direcionada por vítimas específicas e pessoas desaparecidas, prevenção de ameaça específica, substancial e iminente à vida ou à segurança física ou ameaça terrorista, e localização ou identificação de suspeito para investigação, persecução ou execução penal em delitos referidos em anexo e puníveis com pena máxima de ao menos quatro anos, com exigência de que o uso confirme a identidade do indivíduo especificamente visado (União Europeia, 2024)

Assim, a partir dessas perspectivas, entende-se que é possível uma evolução conceitual ao incorporar definições operacionais que o AI Act apresenta para dados biométricos, identificação biométrica, verificação biométrica, sistema de identificação biométrica remota, identificação biométrica remota em tempo real e identificação biométrica remota posterior, inclusive o elemento de ausência de envolvimento ativo do titular e o critério de atraso significativo na distinção entre tempo real e posterior.

Ainda na identificação biométrica remota, o AI Act explicita salvaguardas institucionais que podem orientar o desenho brasileiro para usos admitidos em exceção, como exigência de avaliação de impacto em direitos fundamentais, registro do sistema em base própria, autorização prévia por autoridade judicial ou administrativa independente com decisão vinculante, possibilidade de início sem autorização apenas em urgência com pedido em até 24 horas e dever de interromper o uso e descartar e eliminar dados e resultados quando a autorização for negada, além de vedar decisões com efeito jurídico adverso baseadas exclusivamente na saída do sistema.

O PL, por sua vez, prevê que a utilização de sistemas biométricos para fins de identificação observe princípios e medidas de governança e seja precedida de avaliação de impacto algorítmico, com garantias para exercício de direitos e proteção contra discriminação, e determina descontinuidade do uso quando não houver eliminação ou mitigação substantiva dos riscos, além de estabelecer no setor

público protocolos de acesso e registro de uso, direito à explicação e revisão humanas e publicização de avaliações preliminares.

Nessa comparação, uma possibilidade de aprimoramento orientada pelo AI Act consiste em detalhar, para usos biométricos remotos em exceção, obrigações procedimentais e de supervisão externas ao ente usuário, com registro sistemático e trilha de auditoria, critérios de autorização e deveres de descarte e eliminação associados a negativa ou encerramento da medida.

O AI Act também traz uma vedação que não aparece de modo equivalente no PL ao proibir sistemas que criem ou ampliem bases de reconhecimento facial por coleta não direcionada de imagens faciais na internet ou em imagens de CCTV, o que fecha a porta para a formação de bancos biométricos a partir de extração massiva sem alvo definido. A partir desse parâmetro, o PL pode incorporar uma cláusula específica para impedir a criação e expansão de bases biométricas faciais por raspagem não direcionada, com redação que cubra tanto fontes abertas quanto imagens de videomonitoramento, de modo compatível com a LGPD e com o regime de proteção de dados sensíveis.

Outra diferença se concentra em sistemas de reconhecimento de emoções. O PL classifica como de alto risco os sistemas de identificação e autenticação biométrica destinados ao reconhecimento de emoções, ressalvando a autenticação cujo único objetivo seja a confirmação de pessoa singular específica, o que aciona obrigações gerais do regime de alto risco e de governança. Já o AI Act veda sistemas destinados a inferir emoções na área do trabalho e em instituições de educação, exceto quando o uso se destina a razões médicas ou de segurança, e ainda define sistema de reconhecimento de emoções como aquele que identifica ou infere emoções ou intenções com base em dados biométricos.

A partir disso, a elaboração do PL pode considerar uma vedação contextual para reconhecimento de emoções em trabalho e educação, ou, se mantiver a opção por alto risco, pode delimitar hipóteses estritas e finalidades específicas, com exigências adicionais de justificativa, supervisão humana e transparência ao afetado em razão da assimetria nesses ambientes.

Há também um vetor biométrico que o AI Act trata de forma expressa e que o PL ainda não descreve com igual densidade, a categorização biométrica. O AI Act proíbe sistemas de categorização biométrica que, com base em dados biométricos, deduzam ou infiram raça, opiniões políticas, filiação sindical, crenças religiosas ou filosóficas, vida sexual ou orientação sexual, ao mesmo tempo em que define sistema de categorização biométrica como aquele que atribui pessoas naturais a categorias específicas com base em seus dados biométricos, com ressalva de casos ancilares e tecnicamente necessários.

Esse parâmetro oferece ao Brasil uma via adicional, com norma de proibição dirigida a inferências sensíveis a partir de biometria, o que servirá para reduzir ambiguidades quando sistemas biométricos não pretendem identificar nominalmente, mas operam por classificação e inferência, inclusive em ambientes privados e de serviços.

A distinção entre identificação biométrica remota em tempo real e posterior também produz implicações comparativas. A literatura que examina a proposta europeia apontou questionamentos sobre a separação entre tempo real e posterior e sobre a linha entre categorização biométrica e identificação biométrica, com indicação de que a distinção pode gerar arbitrariedade classificatória (Madiega; Mildebrath, 2021 apud Baccarin, 2023).

O AI Act, além de definir o sistema posterior como o remoto que não é em tempo real, registra a necessidade de salvaguardas para usos posteriores e afasta a possibilidade de vigilância indiscriminada e de contornar as condições estritas do tempo real, ao exigir uso direcionado em termos de indivíduos, local e recorte temporal, com base em conjunto fechado de imagens legalmente obtidas.

Nessa linha, o PL pode explicitar como trata a identificação biométrica remota posterior, seja por extensão da disciplina do artigo 13 para além do tempo real, seja por um capítulo próprio de salvaguardas que cubra usos ex post em videomonitoramento e outras bases, com foco na prevenção de varreduras generalizadas e na delimitação de escopo e base de referência.

Por fim, o AI Act oferece uma perspectiva biométrica de arranjo institucional de transparência e prestação de contas que pode ser adaptada ao Brasil. No uso de identificação biométrica remota em tempo real para finalidades de autoridades de aplicação da lei, o regulamento prevê notificação a autoridades de supervisão e relatórios anuais agregados, com publicação pela Comissão de relatórios anuais sobre o uso, sem dados operacionais sensíveis.

No PL, há previsão de publicização de avaliações preliminares de sistemas de alto risco no setor público e de fixação de padrões mínimos de transparência no âmbito federal, além de protocolos de acesso e de registro de uso e direito à explicação e revisão humanas.

A partir desse contraste, é possível combinar o modelo brasileiro de avaliação e transparência administrativa com um cadastro nacional de usos biométricos remotos e com obrigações periódicas de reporte agregado, o que amplia rastreabilidade pública sem expor informação operacional sensível, sobretudo em contextos de segurança e controle de fronteiras.

REFERÊNCIAS

BRASIL. Autoridade Nacional de Proteção de Dados. **Análise Preliminar do Projeto de Lei (PL) nº 2338/2023.** Brasília, DF: ANPD, 6 jul. 2023a. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/analise-preliminar-do-pl-2338_2023 formatado-ascom.pdf. Acesso em: 22 dez. 2025.

BRASIL. Senado Federal. **Projeto de Lei n.º 2.338, de 2023**. Dispõe sobre o uso da Inteligência Artificial. DF: Senado Federal, 2023. em: https://www25.senado.leg.br/web/atividade/materias/-/materia/157233. Acesso em: 20 dez. 2025.

CANUTO, A. M. de P. Ética no Uso de Dados Biométricos: Histeria ou Uma Preocupação Coerente?. **Computação Brasil**, *[S. l.]*, n. 47, p. 36–39, 2022. DOI: 10.5753/compbr.2022.47.4406. Disponível em: https://journals-sol.sbc.org.br/index.php/comp-br/article/view/4406. Acesso em: 18 dez. 2025.

Coalizão Direitos na Rede. **Posicionamento sobre o PL 2338/2020 e sistemas de identificação biométrica (reconhecimento facial)**. 8 dez. 2025. Disponível em: <**https://direitosnarede.org.br/2025/12/08/posicionamento-pl-2338-sistemas-identificacao-biometrica-reconhecimento-facial/\>**. Acesso em: 22 dez. 2025.

CORRÊA, Adriana Espíndola; LOUREIRO, Maria Fernanda Battaglin. Biometria, autodeterminação informativa e proteção de dados pessoais. **Revista de Direito Civil Contemporâneo**, v. 36, p. 47-74, 2023.

EPIC – Electronic Privacy Information Center. EPIC awards the Tire Meu Rosto da Sua Mira campaign as EPIC International Privacy Champions. Washington, DC, 29 maio 2024. Disponível em: <**https://epic.org/epic-awards-the-tire-meu-rosto-da-sua-mira-campaign-as-epic-international-privacy-champions/\>**. Acesso em: 22 dez. 2025

GERCINA, Cristiane. Havan expõe em vídeos "amostradinho do mês" supostos furtos nas lojas. Folha de S.Paulo, São Paulo, 15 out. 2024. Disponível em: <**https://www1.folha.uol.com.br/mercado/2024/10/havan-expoe-em-videos-amostradinho-do-mes-supostos-furtos-nas-lojas.shtml\>**. Acesso em: 22 dez. 2025.

LIMA, Natalie Alves et al. O uso de bancos de dados biométricos civis em investigações criminais: possíveis avanços à luz de direitos e garantias fundamentais. **Revista Jurídica da Seção Judiciária de Alagoas**, v. 1, n. 8, p. 135-152, 2024. Disponível em: https://revista.jfal.jus.br/RJSJAL/article/view/56. Acesso em 18 dez. 2025

SÃO PAULO (Município). Secretaria Municipal de Segurança Urbana. Programa Smart Sampa. São Paulo, 3 jul. 2024. Disponível em: <**https://prefeitura.sp.gov.br/web/seguranca_urbana/w/smart-sampa-2\>**. Acesso em: 22 dez. 2025

SOUZA, Isadora Dar'c Davi; SILVA , Débora Rafaella da Cunha; ALMEIDA , Adriana Conrado de; ANDRADE , Emanuel Savio de Souza. APLICAÇÃO DO ABIS NA IDENTIFICAÇÃO DE VÍTIMAS DE DESASTRES: UTILIZAÇÃO DOS BANCOS DE DADOS BIOMÉTRICOS. **REVISTA DE ESTUDOS INTERDISCIPLINARES**, *[S. l.]*, v. 5, n. 6, p. 227–244, 2023. DOI: 10.56579/rei.v5i6.793. Disponível em: https://revistas.ceeinter.com.br/revistadeestudosinterdisciplinar/article/view/793. Acesso em: 22 dez. 2025.

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). Bruxelas: Parlamento Europeu e do Conselho [2018]. Disponível em: https://eur lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016R0679. Acesso em: 20 dez. 2025.

UNIÃO EUROPEIA. **Regulamento (UE) 2024/1689 do Parlamento Europeu e do Conselho, de 13 de junho de 2024**. Relativo à criação de regras harmonizadas em matéria de inteli-gência artificial e que altera os Regulamentos (CE) n. 300/2008, (UE) n. 167/2013, (UE) n. 168/2013, (UE) 2018/858, (UE) 2018/1139 e (UE) 2019/2144 e as Diretivas 2014/90/UE, (UE) 2016/797 e (UE) 2020/1828 (Regulamento da Inteligência Artificial). Bruxelas: Parla-mento Europeu e do Conselho [2024]. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=OJ:L_202401689. Acesso em: 20 dez. 2025.

VIOLATO, Ricardo Paranhos Velloso; NETO, Mário Uliani; SIMÕES, Flávio Olmos; PEREIRA, Tiago de Freitas; ANGELONI, Marcus de Assis. **BioCPqD: uma base de dados biométricos com amostras de face e voz de indivíduos brasileiros**. Cadernos CPqD Tecnologia, Campinas, v. 9, n. 2, p. 7-18, jul./dez. 2013.

SCHWERTNER, Suélen Domanoski Goivinho. Projeto de lei impõe mais limites à utilização de dados biométricos. Consultor Jurídico, São Paulo, 6 nov. 2025. Disponível em: <**https://www.conjur.com.br/2025-nov-06/o-uso-indiscriminado-de-dados-biometricos-e-o-pl-2-379-2025/\>**. Acesso em: 22 dez. 2025.