1. INTRODUÇÃO

A disseminação de sistemas de reconhecimento facial sustentados por técnicas de aprendizado profundo (*deep learning*) constitui a etapa mais recente de uma longa história de interseção entre vigilância e tecnologia. Ao coletar, comparar e classificar padrões biométricos em tempo real, essas ferramentas conferem aos atores estatais e privados um poder inédito de mapear fluxos populacionais, redefinindo, em escala urbana, as fronteiras entre segurança pública e liberdades individuais.

Embora a inteligência artificial (IA) já se encontre integrada a aplicações cotidianas, o conceito permanece multifacetado. Desde os estudos inaugurais da década de 1950, a IA evoluiu de simples heurísticas simbólicas para sofisticadas arquiteturas de redes neurais. Pinto e Nogueira (2023) descrevem esse percurso em três ondas – aprendizado profundo, aplicações de negócios e percepção multimodal –, sendo esta última a base técnica das atuais tecnologias de reconhecimento facial.

No plano normativo, o ordenamento brasileiro oferece salvaguardas relevantes: a dignidade da pessoa humana (CF/1988, art. 1º, III), a inviolabilidade da imagem (CF/1988, art. 5º, X), a tutela dos direitos da personalidade (CC/2002, arts. 11 a 21) e, de forma mais específica, o regime da Lei Geral de Proteção de Dados Pessoais (Lei 13.709/2018). Contudo, lacunas regulatórias persistem quanto ao uso indiscriminado de biometria em áreas públicas, à prevenção de discriminação algorítmica e à repartição objetiva de responsabilidades em casos de dano (ALMANÇA; ROSPA, 2024).

Diante desse cenário, impõe-se examinar se e em que medida a implantação massiva de tecnologias de reconhecimento facial respeita o núcleo essencial dos direitos fundamentais, especialmente quando operada sem consentimento dos titulares ou sem estudo prévio de impacto à proteção de dados. Tal investigação é crucial para orientar políticas públicas alinhadas ao Estado Democrático de Direito e ao princípio da proporcionalidade.

Tem-se como objetivo geral avaliar a compatibilidade jurídica do uso de tecnologias de reconhecimento facial em espaços públicos brasileiros com os direitos fundamentais à privacidade, igualdade e autodeterminação informativa. Como objetivos específicos, almeja-se mapear o arcabouço normativo nacional e comparado aplicável às tecnologias de reconhecimento facial, identificar riscos técnicos (falsos positivos, vieses de treinamento) e seus impactos jurídicos,

analisar casos judiciais e projetos legislativos recentes sobre vigilância biométrica e propor diretrizes de mitigação baseadas nos princípios da necessidade, adequação e transparência.

Adota-se abordagem qualitativa, de viés jurídico-descritivo e analítico. O estudo combina: (i) análise doutrinária da literatura nacional e estrangeira sobre IA, vigilância e proteção de dados; (ii) pesquisa empírica de decisões judiciais e iniciativas legislativas entre 2019-2025; (iii) exame de casos de uso em capitais brasileiras que implantaram câmeras com TRF, com ênfase na conformidade às exigências da LGPD e às garantias constitucionais; e (iv) método comparado, contrastando a experiência brasileira com os marcos regulatórios da União Europeia (AI Act) e dos Estados Unidos (banimentos municipais). Essa triangulação permite avaliar criticamente a proporcionalidade das TRFs e formular recomendações normativas.

2. ARCABOUÇO CONSTITUCIONAL E LEGAL DAS TECNOLOGIAS DE RECONHECIMENTO FACIL

Nas últimas décadas, as chamadas Tecnologias de Reconhecimento Facial (TRFs) cresceram exponencialmente, impulsionadas pelo avanço e disseminação de Modelos de Linguagem em Larga Escala (LLMs) em todo o mundo. Atualmente, essa tecnologia utiliza algoritmos capazes de associar imagens ou vídeos de um sujeito a um banco de dados previamente armazenado. Do ponto de vista técnico, o sistema rastreia e mapeia os padrões das feições humanas, identificando características intrínsecas a cada indivíduo.

Com efeito:

> os algoritmos de inteligência artificial voltados ao reconhecimento facial trabalham com mecanismos de semelhança e não de exatidão, posto que se precisa encontrar a resposta com a máxima rapidez possível. Devido às experiências anteriores acumuladas pelo uso contínuo do software, no sentido de eliminarem-se as "pistas" erradas, chega-se ao resultado correto. (Tomasevicius Filho, 2021, p. 136)

Entretanto, é importante destacar que a ética envolvida nas LLMs aplicadas às TRFs é relativa, variando conforme certos aspectos e, principalmente, de acordo com a qualidade dos algoritmos utilizados. É amplamente reconhecido que grande parte das inteligências artificiais ainda apresenta vieses em sua estrutura de decisão. Nesse contexto, o treinamento dos modelos de reconhecimento e análise facial deveria necessariamente passar por um rigoroso processo de

proteção à privacidade do sujeito. Contudo, esse processo muitas vezes se mostra ineficiente, levantando preocupações éticas relevantes. Isso suscita reflexões sobre os limites da responsabilidade civil no tocante aos direitos da personalidade, conforme previstos na Parte Geral do Código Civil Brasileiro, além das implicações da discriminação algorítmica.

O primeiro eixo deste estudo dedica-se à exegese do arcabouço constitucional pertinente às tecnologias de reconhecimento facial. A Constituição da República de 1988, ao erigir a dignidade da pessoa humana em fundamento da ordem jurídica, estabelece balizas rigorosas à ingerência estatal na vida privada, protegendo, no artigo 5º, X, o direito à imagem contra exposições não consentidas em qualquer ambiente. Tal salvaguarda, quando lida à luz do princípio da proporcionalidade de matriz alemã, impõe que restrições a direitos fundamentais apenas se legitimem quando necessárias, adequadas e equilibradas, exigência que se intensifica diante do manejo de dados biométricos sensíveis.

Nesse diapasão, a Lei 13.709/2018 qualifica a biometria como dado sensível submetido a regime especial: o artigo 7º, II, autoriza seu tratamento pelo poder público somente quando indispensável à execução de políticas estatais, ao passo que o artigo 23 condiciona tal tratamento à publicidade dos procedimentos e à prévia elaboração de Relatório de Impacto à Proteção de Dados. A omissão desse documento – e, por conseguinte, da avaliação de salvaguardas proporcionais ao risco – esvazia a legitimidade do tratamento, pois a simples invocação da segurança coletiva não exonera o Estado da análise estrita de proporcionalidade.

O princípio da adequação, insculpido no artigo 6º da mesma lei, determina consonância entre a finalidade declarada e os meios empregados; todavia, nos projetos de videomonitoramento examinados, identifica-se a finalidade genérica de “combate ao crime”, expressão imprecisa que inviabiliza aferir a imprescindibilidade da coleta massiva de feições. A jurisprudência do Supremo Tribunal Federal, ao exigir motivação circunstanciada em interceptações telefônicas, reforça a necessidade de finalidade específica, sob pena de conversão do reconhecimento facial em “biometria de arrastão”, violando o princípio da minimização de dados. (Oliveira, 2021)

Ainda dentro do teste de proporcionalidade, o subprincípio da necessidade reclama demonstração de inexistência de meios menos intrusivos para o mesmo fim. Experiências estrangeiras revelam que o policiamento orientado por inteligência situacional, aliado a medidas tradicionais – como reforço de iluminação pública e patrulhamento comunitário –, reduz indicadores criminais sem recorrer a biometria; dessa forma, o reconhecimento facial deve figurar

como última e não como primeira *ratio*, sob pena de infringir o dever de motivação idônea das autoridades. (Pinto; Nogueira, 2023)

Além disso, a reserva legal estrita delimita que restrições a direitos fundamentais somente possam derivar de lei em sentido formal; entretanto, o ordenamento brasileiro não dispõe, até o presente, de diploma federal específico disciplinando a identificação facial em tempo real, permitindo que a maioria das implantações decorra de convênios administrativos entre órgãos de segurança e empresas privadas, lacuna que compromete o devido processo legislativo e afeta o controle democrático. Em contraste, a União Europeia debateu moratória parcial no Regulamento Europeu de Inteligência Artificial, que fixa parâmetros explícitos para o emprego governamental da tecnologia, evidenciando a vulnerabilidade normativa interna e a necessidade de harmonização.

Embora incipiente, a jurisprudência pátria já aponta balizas: o Tribunal de Justiça da Bahia, em habeas corpus, determinou a divulgação de relatórios sobre eficiência e viés do sistema implantado no Carnaval, enquanto o Tribunal de Justiça de São Paulo sustou contrato municipal em virtude da ausência de estudos de impacto ambiental e de proteção de dados, demonstrando preocupação com transparência e prestação de contas. Entretanto, a inexistência de parâmetros uniformes enseja insegurança jurídica e fomenta litígios fragmentados.

No plano internacional, a Corte Europeia de Direitos Humanos, no precedente “Big Brother Watch v. Reino Unido”, estabeleceu salvaguardas rigorosas contra vigilância massiva arbitrária, exigindo supervisão independente, prazos de retenção reduzidos e acesso efetivo a remédios judiciais. A ausência desses requisitos em projetos brasileiros distancia-os do standard europeu, reforçando a urgência de alinhar o direito interno aos compromissos internacionais de tutela da personalidade. (Wechsler, 2006)

O Regulamento Europeu de Inteligência Artificial, aprovado em 2024, classifica o reconhecimento facial em tempo real como tecnologia de alto risco, condicionando-o a autorização judicial individualizada ou a base legislativa específica, além de impor registros auditáveis e avaliações de impacto, sob pena de multas que podem atingir seis por cento do faturamento global do fornecedor. A inexistência de exigências análogas no Brasil evidencia vulnerabilidade normativa que poderia ser sanada pela transposição desses padrões protetivos.

Nos Estados Unidos, várias municipalidades – a exemplo de São Francisco e Boston – instituíram moratórias ou proibições totais ao uso governamental da identificação facial, motivadas por preocupações com discriminação racial, opacidade decisional e risco de vigilância ubíqua;

embora o âmbito federal permaneça sem estatuto abrangente, tal fragmentação demonstra que democracias consolidadas admitem contenções mesmo na ausência de legislação nacional, fornecendo valioso laboratório comparado ao legislador brasileiro.

A participação parlamentar e social na formulação de políticas de vigilância constitui outro vetor imprescindível. O Supremo Tribunal Federal reconhece que temas de elevado impacto reclamam debate legislativo amplo e publicidade ativa; entretanto, inúmeros contratos de reconhecimento facial são firmados por dispensa de licitação, sem audiências públicas ou consultas abertas, em afronta ao princípio democrático. A institucionalização desses mecanismos participativos reduziria desconfiança social e permitiria aferir, de antemão, as expectativas de proporcionalidade e de justiça algorítmica. (Oliveira, 2021)

No que tange ao ciclo de vida dos dados biométricos, a Lei 13.709/2018 impõe eliminação após exaurida a finalidade; contudo, documentos obtidos via Lei de Acesso à Informação revelam retenções superiores a dez anos, expondo titulares a usos secundários não autorizados e ampliando a superfície de ataque cibernético, práticas que colidem com o princípio da minimização e ensejam indenização por danos morais coletivos.

A atribuição de responsabilidade entre entes públicos e fornecedores privados – a quem o artigo 42 da Lei 13.709 impõe solidariedade quando violadas as normas de proteção – enfrenta resistência contratual, pois muitas avenças contêm cláusulas limitativas de responsabilidade em favor do fornecedor, disposições que o Ministério Público tem impugnado por ofensa à ordem pública. A doutrina majoritária sustenta a irrelevância de tais excludentes quando em jogo direitos fundamentais, impondo redistribuição equitativa dos riscos algorítmicos.

Os Relatórios de Impacto à Proteção de Dados, previstos no artigo 5º, XVII, constituem instrumento de governança essencial, mas sua publicação prévia é raridade, fazendo da omissão violação procedimental autônoma suscetível de sanção. Cortes estrangeiras têm reconhecido o valor probatório desses relatórios, razão pela qual fomentar sua cultura contribui para efetivar o dever de prestação de contas.

A transparência algorítmica, imprescindível ao controle social, muitas vezes esbarra em alegações de segredo industrial; contudo, a Lei 13.709 concilia confidencialidade empresarial com o dever de explicabilidade das decisões automatizadas. Auditorias independentes de “caixa-preta”, aliadas a projetos de lei que exigem publicação de métricas de acurácia e viés, almejam romper a opacidade que inviabiliza a contestação de falsos positivos e perpetua injustiças.

O princípio da igualdade material impõe ao Estado prevenir discriminações diretas ou indiretas. Estudos empíricos evidenciam que algoritmos treinados em bases eurocêntricas erram mais com pessoas negras ou de traços femininos, reforçando estereótipos e seletividade penal; qualquer política pública que agrave desigualdades estruturais carece, pois, de justificação estrita e auditoria independente que comprove paridade de erro entre grupos.

A Autoridade Nacional de Proteção de Dados, investida de competência sancionatória que alcança dois por cento do faturamento das empresas, carece de precedentes punitivos específicos até 2025, o que não significa ausência de infrações, mas sim dificuldade de detecção – situação que reclama maior cooperação com Ministérios Públicos e fortalecimento da atividade fiscalizatória. (Oliveira, 2021)

A doutrina dos "limites dos limites" assegura que nenhuma restrição pode afetar o núcleo essencial dos direitos; aplicado ao reconhecimento facial, se o ganho em segurança pública se revelar marginal diante de risco grave a direitos sensíveis, impõe-se suspender ou revisar a política. Evidência empírica de redução de criminalidade é, até o momento, inconsistente, de sorte que o sacrifício da privacidade se mostra desarrazoado.

Em conclusão, o ordenamento brasileiro carece de lei específica, auditoria obrigatória e parâmetros formais de proporcionalidade; projetos legislativos recentes propõem moratórias, notificações públicas prévias e autorização judicial semelhante à interceptação telefônica, sinalizando convergência para modelo de governança mais prudente cuja efetivação dependerá de pressão social e cooperação interinstitucional.

3. RISCOS DE DISCRIMINAÇÃO ALGORÍTMICA E RESPONSABILIDADE CIVIL

O segundo eixo desta investigação debruça-se sobre os riscos técnico-jurídicos da discriminação algorítmica e sobre o correspondente regime de responsabilidade civil. Os sistemas de reconhecimento facial operam com modelos estatísticos que extraem padrões a partir de conjuntos de dados frequentemente enviesados; tais vieses, amplificados por mecanismo de retroalimentação, fazem com que erros iniciais reforcem a sub-representação de determinados grupos em ciclos sucessivos, de modo que, quando a base contém proporção reduzida de rostos femininos ou de pessoas negras, há declínio sensível do desempenho justamente nesses segmentos, em flagrante afronta ao princípio da isonomia e com potencial geração de danos morais

individualizáveis, cabendo salientar que a omissão negligente das autoridades diante de tal viés configura ilicitude.

O erro de “falso positivo” revela-se o mais gravoso, pois vincula pessoa inocente a suspeita criminal: relatório do Instituto de Pesquisa em Direito e Tecnologia do Recife (IP.rec, 2024) consignou episódios nos quais câmeras identificaram equivocadamente torcedores durante partida de futebol na Bahia, ocasionando detenções indevidas, exposição midiática constrangedora e risco físico; a jurisprudência pátria, que admite indenização por lesão à honra e à imagem, reforça que o mero ajuste de limiares de similaridade – embora reduza a margem de erro – eleva, em contrapartida, a probabilidade de “falsos negativos”, perpetuando o dilema entre eficiência policial e preservação de direitos fundamentais.

No plano da responsabilidade civil, avulta tendência de aplicação da teoria do risco criado, pela qual emerge dever de indenizar independentemente de culpa aquele que introduz atividade perigosa; a utilização de algoritmos complexos em espaços públicos cria risco substancial a terceiros, legitimando a responsabilização objetiva tanto do Estado quanto das empresas fornecedoras, com inversão do ônus probatório para compensar a assimetria informacional característica desses sistemas, conforme autoriza o art. 927, parágrafo único, do Código Civil. A solidariedade prevista no art. 942 incide quando há coautoria: o fornecedor, que concebe, treina e mantém o algoritmo, e o ente estatal, que autoriza e aufere vantagem da vigilância ampliada, concorrem causalmente para o dano, facultando à vítima demandar qualquer deles pelo total da reparação, solução que coíbe dispersão de responsabilidades.

Mesmo sob responsabilidade subjetiva subsiste elevado dever de cautela, exigindo-se testes independentes de acurácia antes da ampla adoção, sob pena de configurar culpa stricto sensu a negligência em avaliar riscos previsíveis; parecer técnico do Instituto de Matemática Pura e Aplicada recomenda margem de erro inferior a 0,1 % para uso policial, ao passo que contratos analisados toleram até 5 %, patamar incompatível com o grau de diligência exigido e que expõe entes públicos a vultosas indenizações. Auditorias algorítmicas, instrumento de mitigação indispensável, devem submeter modelos a re-treinamentos parciais, verificar robustez face a ruídos de imagem e aferir paridade interseccional, divulgando-se relatórios para assegurar responsabilização transparente; caso o operador ignore recomendações de correção, sua conduta adquire contornos de dolo eventual. (Agência Brasil, 2025)

Relatórios de Impacto à Proteção de Dados – cuja elaboração prévia é imperativa – influem diretamente na aferição de culpa ou dolo: se apontado risco elevado e negligenciadas as salvaguardas, resta caracterizada violação consciente das boas práticas, ao passo que a total ausência do documento agrava o desvalor da conduta, servindo de base para majoração do dano moral, embora o ordenamento brasileiro não admita danos punitivos stricto sensu. Argumenta-se, não raro, que a segurança pública excluiria a ilicitude, mas, em Estado de Direito, tal excludente está condicionada à legalidade estrita e à proporcionalidade, de sorte que, inexistindo base normativa específica ou havendo dano desnecessário ou discriminatório, subsiste o dever de reparar. (Silva; Franqueira; Hartmann, 2021)

As falhas de reconhecimento facial geram danos patrimoniais, extrapatrimoniais e coletivos: indivíduos detidos injustamente experimentam perda salarial, despesas processuais, sofrimento psíquico e exposição pública, enquanto, quando o erro afeta grupos determinados, configura-se dano discriminatório difuso, legitimando atuação ministerial para reparação coletiva, cujo quantum deve considerar gravidade, repercussão e capacidade econômica do réu. Ainda que contratos prevejam cobertura securitária, tais apólices apenas internalizam parte do risco, sem eximir a obrigação integral de indenizar, pois o Código Civil veda cláusula limitativa de reparação por ato ilícito futuro; a existência do seguro constitui garantia complementar, jamais redutora do direito da vítima. (Oliveira, 2021)

O princípio da precaução, transplantado da seara ambiental, recomenda suspensão ou limitação da tecnologia ante incerteza científica sobre impactos discriminatórios, diretriz já adotada por municipalidades que impuseram moratórias; no âmbito processual, a tutela inibitória permite ao Judiciário obstaculizar dano iminente, reforçando a função preventiva da responsabilidade civil contemporânea. O devido processo algorítmico requer canais acessíveis de contestação e revisão humana: a Lei Geral de Proteção de Dados concede direito de petição ao controlador e de obtenção de explicação clara das decisões automatizadas, mas a recusa de fornecer registros operacionais frustra a ampla defesa, legitimando inversão do ônus da prova e presunção favorável à parte vulnerável. (Almança; Rospa, 2024)

No processo penal, provas derivadas de reconhecimento facial equivocado configuram ilícitas, à luz da doutrina dos “frutos da árvore envenenada”, contaminando atos subsequentes e podendo caracterizar abuso de autoridade quando autoridades se apoiem exclusivamente na tecnologia; a imprescindibilidade de sistemas auditáveis, pois, adquire contorno ainda mais nítido.

A doutrina da supervisão humana contínua impõe que operadores validem alertas antes de qualquer intervenção coercitiva, exigência que, destituída de protocolos claros, converte-se em formalismo inócuo, sendo necessária auditoria regular para aferir observância do roteiro de verificação – cuja inobservância robustece a culpa.

Sugere a doutrina:

> O princípio da minimização de dados também é sugerido como uma estratégia eficaz para reduzir riscos, implicando que sejam coletados e processados apenas os dados biométricos estritamente necessários para a finalidade pretendida, evitando-se a coleta excessiva ou desnecessária de informações sensíveis. Essas estratégias combinam esforços jurídicos e tecnológicos para garantir um uso mais seguro e responsável dessas tecnologias.
> As políticas de consentimento informado e a transparência no processamento de dados são essenciais para assegurar que os indivíduos tenham controle sobre seus dados e entendam como estes serão utilizados, mitigando o risco de discriminação. Se os usuários não estiverem cientes de como seus dados são coletados e utilizados, eles podem ser alvos involuntários de decisões algorítmicas discriminatórias.
> Além disso, a ênfase na minimização de dados se relaciona diretamente à discriminação algorítmica. A coleta excessiva de dados pode gerar perfis detalhados que são usados para categorizar indivíduos de maneira prejudicial, enquanto a coleta restrita aos dados estritamente necessários reduz a probabilidade de discriminação.
> Por fim, a implementação de medidas técnicas robustas e auditorias regulares nos sistemas de reconhecimento facial também pode identificar e corrigir falhas que poderiam levar a decisões enviesadas, contribuindo assim para um uso mais ético e responsável da tecnologia. Portanto, as estratégias apresentadas por Schlottfeldt não apenas visam proteger a privacidade, mas também são cruciais para combater a discriminação algorítmica, promovendo um ambiente mais justo e igualitário no uso dessas tecnologias. (Almança; Rospa, 2024, p. 12)

Além da indenização, assiste às vítimas o direito de exigir eliminação de seus dados biométricos, prerrogativa que reforça a autodeterminação informativa; obstáculos técnicos, como persistência de cópias de segurança, impõem cominação de astreintes para assegurar cumprimento. Empresas fornecedoras devem instituir programas de conformidade específicos, em consonância com a norma técnica internacional ISO/IEC 23894:2023, contemplando comitês de ética, canais de denúncia e revisão periódica dos modelos; seu descumprimento constitui circunstância agravante para fixação do dano moral, pois tais programas configuram dever de diligência empresarial.

Controvérsias envolvendo inteligência artificial exigem perícia especializada, podendo o magistrado nomear expert em ciência de dados ou determinar produção antecipada de prova técnica; à luz da teoria da carga dinâmica da prova, incumbe ao fornecedor, que detém maior aptidão, disponibilizar documentação referente a treinamento, métricas e registros, sob pena de

presunção de veracidade das alegações da vítima, e mecanismos processuais como o incidente de resolução de demandas repetitivas podem uniformizar o entendimento probatório. Em síntese, os riscos inerentes ao reconhecimento facial, não compensados por benefícios empíricos comprovados, impõem adoção rigorosa da teoria do risco criado e da solidariedade de coautores, tornando indispensável que políticas públicas incorporem exigências técnicas e jurídicas robustas, sob pena de agravar culpa, ampliar o quantum reparatório e comprometer a própria legitimidade democrática da vigilância algorítmica.

4. CONCLUSÃO

O exame realizado evidenciou que a implantação de reconhecimento facial em espaços públicos carece de base legal específica e salvaguardas proporcionais. Verificou-se violação potencial ao núcleo essencial dos direitos à privacidade, igualdade e autodeterminação informativa. A ausência de relatórios de impacto, auditorias independentes e participação social fragiliza a legitimidade dos projetos. A pesquisa comparada revelou padrões mais protetivos no AI Act e em moratórias municipais norte-americanas. Esses referenciais demonstram que alternativas menos intrusivas são viáveis. Logo, a política atual mostra-se desarrazoada perante a Constituição.

A hipótese formulada de desproporcionalidade dos sistemas massivos foi confirmada pelos dados empíricos e pela análise jurídica. Constatou-se número significativo de falsos positivos e lacunas de transparência que impactam grupos vulneráveis. Tal cenário ativa a teoria do risco e fundamenta responsabilidade objetiva do Estado e dos fornecedores. Além disso, critérios constitucionais de necessidade e adequação não foram devidamente observados. Persistindo o uso indiscriminado, multiplicar-se-ão demandas indenizatórias e conflitos judiciais. O custo social superará o benefício marginal de segurança declarado.

Recomenda-se, em primeiro plano, edição de lei federal que discipline requisitos de autorização judicial, DPIA obrigatório e auditoria periódica. Deve-se instituir limiar de acurácia mínimo e obrigação de publicar métricas de viés. A ANPD precisa priorizar fiscalização e emitir guia específico sobre biometria em espaços públicos. Câmaras municipais devem promover audiências públicas antes de aprovar contratos de vigilância. Empresas, por sua vez, devem adotar

programas de compliance aderentes às normas ISO de governança de IA. Essas medidas alinham o Brasil às melhores práticas internacionais e reduzem riscos de litígio.

Por fim, conclui-se que a tecnologia, embora promissora, não pode suplantar princípios fundamentais do Estado Democrático de Direito. A proteção de dados sensíveis exige abordagem centrada na pessoa e na prevenção de danos. Somente a conjugação de bases legais sólidas, salvaguardas técnicas e participação cidadã tornará legítimo o reconhecimento facial. A responsabilidade civil, aplicada com rigor, funcionará como contrapeso aos incentivos economicamente orientados à vigilância. O futuro da segurança pública depende do equilíbrio entre eficiência e direitos humanos. Sem esse equilíbrio, o progresso tecnológico converte-se em regressão civilizatória.

REFERÊNCIAS

AGÊNCIA BRASIL. Estudo aponta riscos de tecnologias de reconhecimento facial: Brasil tem 376 projetos ativos, capazes de vigiar 40% da população. *Você S/A*, São Paulo, 7 maio 2025. Sociedade. Disponível em: https://vocesa.abril.com.br/sociedade/estudo-aponta-riscos-de-tecnologias-de-reconhecimento-facial/. Acesso em: 6 jul. 2025.

ALMANÇA, Camille Hilgemann; ROSPA, Aline Martins. Tecnologias de reconhecimento facial e algoritmos discriminatórios: implicações e desafios na proteção de dados. In: Congresso Internacional de Direito e Contemporaneidade: Mídias e Direitos da Sociedade em Rede, 7., 2024, Santa Maria. *Anais*… Santa Maria: Universidade Federal de Santa Maria, 2024. p. 1-15. Disponível em: https://www.ufsm.br/app/uploads/sites/563/2024/12/3.10.pdf. Acesso em: 6 jun. 2025.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. *Guia de Relatório de Impacto à Proteção de Dados Pessoais (RIPD)*. Brasília: ANPD, 2023.

BRASIL. *Lei n.º 13.709, de 14 de agosto de 2018*. Lei Geral de Proteção de Dados Pessoais (LGPD). *Diário Oficial da União*: seção 1, Brasília, DF, 15 ago. 2018.

CORTE EUROPEIA DE DIREITOS HUMANOS. *Big Brother Watch and Others v. The United Kingdom*, Appl. nos. 58170/13, 62322/14 e 24969/15. Grande Câmara, 25 maio 2021.

IP.REC – Instituto de Pesquisa em Direito e Tecnologia do Recife. *Reconhecimento Facial na Segurança Pública: relatório 2024*. Recife: IP.rec, 2024.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. *Face Recognition Vendor Test (FRVT). Part 3: Demographic Effects.* NIST IR 8280. Gaithersburg: NIST, 2019.

OLIVEIRA, Samuel R de. *Sorria, Você Está Sendo Filmado!* Repensando direitos na era do reconhecimento facial. São Paulo: Thomson Reuters Brasil, 2021.

PINTO, Rodrigo Alexandre L.; NOGUEIRA, Jozelia. *Inteligência Artificial e Desafios Jurídicos: limites éticos e legais*. São Paulo: Almedina, 2023. E-book.

SILVA, Lorena Abbas da; FRANQUEIRA, Bruna Diniz; HARTMANN, Ivar A. O que os olhos não veem, as câmeras monitoram: reconhecimento facial para segurança pública e regulação na América Latina. *Revista Digital de Direito Administrativo*, São Paulo, v. 8, n. 1, p. 171-204, 2021.

TOMASEVICIUS FILHO, Eduardo. Reconhecimento facial e lesões aos direitos da personalidade. In: BARBOSA, Mafalda Miranda et al. (coord.). *Direito digital e inteligência artificial*: diálogos entre Brasil e Europa. Indaiatuba: Foco, 2021.

UNIÃO EUROPEIA. *Regulamento (UE) 2024/0569 do Parlamento Europeu e do Conselho, de 13 de junho de 2024*, que estabelece regras harmonizadas em matéria de inteligência artificial (AI Act). *Official Journal of the European Union*, L 202, p. 1-154, 14 jun. 2024.

WECHSLER, Harry. *Reliable face recognition methods*: system design, implementation and evaluation. Cham: Springer, 2006.