VI CONGRESSO INTERNACIONAL DE DIREITO E INTELIGÊNCIA ARTIFICIAL (VI CIDIA)

PRIVACIDADE, PROTEÇÃO DE DADOS PESSOAIS E NEGÓCIOS INOVADORES II

P961
Privacidade, proteção de dados pessoais e negócios inovadores II [Recurso eletrônico on-line] organização VI Congresso Internacional de Direito e Inteligência Artificial (VI CIDIA): Skema Business School – Belo Horizonte;

Coordenadores: Alexandre Schmitt da Silva Mello, Mariana de Moraes Palmeira e Pietra Daneluzzi Quinelato – Belo Horizonte: Skema Business School, 2025.

Inclui bibliografia
ISBN: 978-65-5274-361-9
Modo de acesso: www.conpedi.org.br em publicações
Tema: Perspectivas globais para a regulação da inteligência artificial.
1. GDPR. 2. Segurança da informação. 3. Compliance. I. VI Congresso Internacional de Direito e Inteligência Artificial (1:2025 : Belo Horizonte, MG).

CDU: 34

VI CONGRESSO INTERNACIONAL DE DIREITO E INTELIGÊNCIA ARTIFICIAL (VI CIDIA)

PRIVACIDADE, PROTEÇÃO DE DADOS PESSOAIS E NEGÓCIOS INOVADORES II

Apresentação

A SKEMA Business School é uma organização francesa sem fins lucrativos, com presença em sete países diferentes ao redor do mundo (França, EUA, China, Brasil, Emirados Árabes Unidos, África do Sul e Canadá) e detentora de três prestigiadas acreditações internacionais (AMBA, EQUIS e AACSB), refletindo seu compromisso com a pesquisa de alta qualidade na economia do conhecimento. A SKEMA reconhece que, em um mundo cada vez mais digital, é essencial adotar uma abordagem transdisciplinar.

Cumprindo esse propósito, o VI Congresso Internacional de Direito e Inteligência Artificial (VI CIDIA), realizado nos dias 18 e 19 de setembro de 2025, em formato híbrido, manteve-se como o principal evento acadêmico sediado no Brasil com o propósito de fomentar ricas discussões sobre as diversas interseções entre o direito e a inteligência artificial. O evento, que teve como tema central a "Regulação da Inteligência Artificial", contou com a presença de renomados especialistas nacionais e internacionais, que abordaram temas de relevância crescente no cenário jurídico contemporâneo.

Profissionais e estudantes dos cursos de Direito, Administração, Economia, Ciência de Dados, Ciência da Computação, entre outros, tiveram a oportunidade de se conectar e compartilhar conhecimentos, promovendo um ambiente de rica troca intelectual. O VI CIDIA contou com a participação de acadêmicos e profissionais provenientes de diversas regiões do Brasil e do exterior. Entre os estados brasileiros representados, estavam: Alagoas (AL), Bahia (BA), Ceará (CE), Goiás (GO), Maranhão (MA), Mato Grosso do Sul (MS), Minas Gerais

Foram discutidos assuntos variados, desde a própria regulação da inteligência artificial, eixo central do evento, até as novas perspectivas de negócios e inovação, destacando como os algoritmos estão remodelando setores tradicionais e impulsionando a criação de empresas inovadoras. Com uma programação abrangente, o congresso proporcionou um espaço vital para discutir os desafios e oportunidades que emergem com o desenvolvimento algorítmico, reforçando a importância de uma abordagem jurídica e ética robusta nesse contexto em constante evolução.

A programação teve início às 13h, com o check-in dos participantes e o aquecimento do público presente. Às 13h30, a abertura oficial foi conduzida pela Prof.ª Dr.ª Geneviève Poulingue, que, em sua fala de boas-vindas, destacou a relevância do congresso para a agenda global de inovação e o papel da SKEMA Brasil como ponte entre a academia e o setor produtivo.

Em seguida, às 14h, ocorreu um dos momentos mais aguardados: a Keynote Lecture do Prof. Dr. Ryan Calo, renomado especialista internacional em direito e tecnologia e professor da University of Washington. Em uma conferência instigante, o professor explorou os desafios metodológicos da regulação da inteligência artificial, trazendo exemplos de sua atuação junto ao Senado dos Estados Unidos e ao Bundestag alemão.

A palestra foi seguida por uma sessão de comentários e análise crítica conduzida pelo Prof. Dr. José Luiz de Moura Faleiros Júnior, que contextualizou as reflexões de Calo para a realidade brasileira e fomentou o debate com o público. O primeiro dia foi encerrado às 14h50 com as considerações finais, deixando os participantes inspirados para as discussões do dia seguinte.

As atividades do segundo dia tiveram início cedo, com o check-in às 7h30. Às 8h20, a Prof.ª Dr.ª Margherita Pagani abriu a programação matinal com a conferência Unlocking Business Creativity Using Artificial Intelligence, apresentando insights sobre como a IA pode

Após um breve e merecido coffee break às 9h40, os participantes retornaram para uma manhã de intensas reflexões. Às 10h30, o pesquisador Prof. Dr. Steve Ataky apresentou a conferência Regulatory Perspectives on AI, compartilhando avanços e desafios no campo da regulação técnica e ética da inteligência artificial a partir de uma perspectiva global.

Encerrando o ciclo de palestras, às 11h10, o Prof. Dr. Filipe Medon trouxe ao público uma análise profunda sobre o cenário brasileiro, com a palestra AI Regulation in Brazil. Sua exposição percorreu desde a criação do Marco Legal da Inteligência Artificial até os desafios atuais para sua implementação, envolvendo aspectos legislativos, econômicos e sociais.

Nas tardes dos dois dias, foram realizados grupos de trabalho que contaram com a apresentação de cerca de 60 trabalhos acadêmicos relacionados à temática do evento. Com isso, o evento foi encerrado, após intensas discussões e troca de ideias que estabeleceram um panorama abrangente das tendências e desafios da inteligência artificial em nível global.

Os GTs tiveram os seguintes eixos de discussão, sob coordenação de renomados especialistas nos respectivos campos de pesquisa:

a) Startups e Empreendedorismo de Base Tecnológica – Coordenado por Allan Fuezi de Moura Barbosa, Laurence Duarte Araújo Pereira, Cildo Giolo Júnior, Maria Cláudia Viana Hissa Dias do Vale Gangana e Yago Oliveira

b) Jurimetria Cibernética Jurídica e Ciência de Dados – Coordenado por Arthur Salles de Paula Moreira, Gabriel Ribeiro de Lima, Isabela Campos Vidigal Martins, João Victor Doreto e Tales Calaza

c) Decisões Automatizadas e Gestão Empresarial / Algoritmos, Modelos de Linguagem e Propriedade Intelectual – Coordenado por Alisson Jose Maia Melo, Guilherme Mucelin e

f) Regulação da Inteligência Artificial – III – Coordenado por Ana Júlia Silva Alves Guimarães, Erick Hitoshi Guimarães Makiya, Jessica Fernandes Rocha, João Alexandre Silva Alves Guimarães e Luiz Felipe Vieira de Siqueira

g) Inteligência Artificial, Mercados Globais e Contratos – Coordenado por Gustavo da Silva Melo, Rodrigo Gugliara e Vitor Ottoboni Pavan

h) Privacidade, Proteção de Dados Pessoais e Negócios Inovadores – I – Coordenado por Dineia Anziliero Dal Pizzol, Evaldo Osorio Hackmann, Gabriel Fraga Hamester, Guilherme Mucelin e Guilherme Spillari Costa

i) Privacidade, Proteção de Dados Pessoais e Negócios Inovadores – II – Coordenado por Alexandre Schmitt da Silva Mello, Lorenzzo Antonini Itabaiana, Marcelo Fonseca Santos, Mariana de Moraes Palmeira e Pietra Daneluzzi Quinelato

j) Empresa, Tecnologia e Sustentabilidade – Coordenado por Marcia Andrea Bühring, Ana Cláudia Redecker, Jessica Mello Tahim e Maraluce Maria Custódio.

Cada GT proporcionou um espaço de diálogo e troca de experiências entre pesquisadores e profissionais, contribuindo para o avanço das discussões sobre a aplicação da inteligência artificial no direito e em outros campos relacionados.

Um sucesso desse porte não seria possível sem o apoio institucional do Conselho Nacional de Pesquisa e Pós-graduação em Direito - CONPEDI, que desde a primeira edição do evento provê uma parceria sólida e indispensável ao seu sucesso. A colaboração contínua do CONPEDI tem sido fundamental para a organização e realização deste congresso, assegurando a qualidade e a relevância dos debates promovidos.

Reitora – SKEMA Business School - Campus Belo Horizonte

Prof. Ms. Dorival Guimarães Pereira Júnior

Coordenador do Curso de Direito – SKEMA Law School

Prof. Dr. José Luiz de Moura Faleiros Júnior

Coordenador de Pesquisa – SKEMA Law School

VIGILÂNCIA ALGORÍTMICA E DISCRIMINAÇÃO ABUSIVA: UMA ANÁLISE DO SISTEMA SMART SAMPA À LUZ DO PRINCÍPIO DA NÃO DISCRIMINAÇÃO DA LGPD (ART. 6º, IX)

ALGORITHMIC SURVEILLANCE AND ABUSIVE DISCRIMINATION: AN ANALYSIS OF THE SMART SAMPA SYSTEM IN LIGHT OF THE LGPD'S NONDISCRIMINATION PRINCIPLE (ART.6,IX)

Charles Glauber da Costa Pimentel [1]

Resumo

Este artigo analisa criticamente o programa SMART SAMPA, sistema de vigilância algorítmica baseado em reconhecimento facial, investigando suas inconsistências operacionais e a possibilidade de caracterização de discriminação abusiva conforme o art. 6º, inciso IX, da Lei Geral de Proteção de Dados (LGPD). Com base no Relatório de Transparência (novembro de 2024 a maio de 2025), identificam-se falhas como falsos positivos, inconsistências cadastrais e ausência de atualização no Banco Nacional de Mandados de Prisão (BNMP), que resultaram em abordagens indevidas e violações de direitos fundamentais. A pesquisa adota uma abordagem jurídico-dogmática, enriquecida com análise documental e teorias críticas da vigilância de Foucault e Han, destacando os riscos sistêmicos das tecnologias preditivas na segurança pública.

Palavras-chave: Vigilância algorítmica, Lgpd, Discriminação abusiva, Reconhecimento facial, Direitos fundamentais

Abstract/Resumen/Résumé

This article critically examines the SMART SAMPA program, an algorithmic surveillance system based on facial recognition, focusing on its operational inconsistencies and the potential qualification as abusive discrimination under Article6, itemIX, of Brazil's General Data Protection Law (LGPD). Drawing on the Transparency Report (November2024 to May2025), the study highlights failures such as false positives, data inconsistencies, and the lack of updates in the National Warrant Database (BNMP), which resulted in unwarranted

1 INTRODUÇÃO

Desenvolvido no âmbito das discussões contemporâneas sobre inteligência artificial e proteção de dados pessoais, este artigo está inserido na linha de pesquisa Privacidade, Proteção de Dados Pessoais e Negócios Inovadores, conforme proposta do VI Congresso Internacional de Direito e Inteligência Artificial (VI CIDIA). O objetivo central da pesquisa é analisar em que medida as inconsistências operacionais do programa SMART SAMPA, especialmente os falsos positivos decorrentes do uso de reconhecimento facial, podem configurar uma forma de discriminação abusiva no que diz respeito à violação ao princípio da não discriminação previsto no art. 6º, inciso IX da Lei n.º 13.709/2018 (Lei Geral de Proteção de Dados Pessoais – LGPD).

Este estudo analisa criticamente como as falhas identificadas no SMART SAMPA, implementado na cidade de São Paulo, podem gerar impactos sobre direitos fundamentais, como a privacidade, a dignidade da pessoa humana e a presunção de inocência. A investigação está ancorada no cruzamento entre tecnologia, direitos fundamentais e governança de dados, com ênfase na necessidade de auditoria algorítmica e de políticas públicas que minimizem práticas discriminatórias. A análise do Relatório de Transparência do SMART SAMPA, referente ao período de novembro de 2024 a maio de 2025, evidencia falhas como falsos positivos, inconsistências cadastrais e falta de atualização no Banco Nacional de Mandados de Prisão (BNMP), situações que impactam diretamente os cidadãos.

A questão central que norteia esta pesquisa é: de que forma as inconsistências operacionais do SMART SAMPA podem configurar discriminação abusiva em violação ao art. 6º, inciso IX da LGPD? Para responder a essa indagação, o objetivo geral consiste em analisar como as inconsistências do sistema, sobretudo os falsos positivos de reconhecimento facial, configuram tratamento discriminatório abusivo de dados pessoais sensíveis, à luz do art. 6º, IX da LGPD, e seus impactos nos direitos fundamentais. Os objetivos específicos são: (i) contextualizar a evolução histórica e teórica da vigilância, com base em Foucault e Han; (ii) Delimitar e explicitar o conteúdo dos princípios da LGPD, com ênfase no art. 6º, IX, bem como sua aplicabilidade ao reconhecimento facial; (iii) Iientificar e qualificar as inconsistências apontadas no Relatório de Transparência do SMART SAMPA; (iv) demonstrar e explicar os mecanismos pelos quais tais inconsistências caracterizam discriminação algorítmica abusiva e seus efeitos sobre direitos fundamentais.

A relevância da pesquisa reside na urgência de compreender criticamente os efeitos sociais e jurídicos de sistemas de vigilância algorítmica, que, quando implementados sem mecanismos de governança, podem perpetuar desigualdades e afetar garantias constitucionais.

O caso SMART SAMPA oferece um exemplo empírico significativo para analisar os limites éticos e legais da inteligência artificial aplicada à segurança pública.

A metodologia adotada é de natureza jurídico-dogmática e qualitativa, com análise normativa da LGPD e de seus princípios; revisão bibliográfica de autores de referência, como Foucault, Han e Doneda; e análise documental do Relatório de Transparência do SMART SAMPA. A pesquisa adota ainda uma abordagem crítica acerca dos vieses algorítmicos e da responsabilidade do poder público no tratamento de dados sensíveis.

O artigo está estruturado em quatro seções de desenvolvimento, além desta introdução e das considerações finais. A Seção 2 expõe os fundamentos teóricos da vigilância e do controle social, do panoptismo foucaultiano à sociedade da transparência de Han, introduzindo a vigilância algorítmica. A Seção 3 examina a LGPD e os direitos fundamentais no contexto da vigilância, detalhando princípios aplicáveis, o regime dos dados sensíveis, a exceção do art. 4º e o papel da ANPD. A Seção 4 descreve o funcionamento do SMART SAMPA e analisa suas inconsistências operacionais (falsos positivos, falhas cadastrais e desatualização do BNMP) e o potencial discriminatório decorrente da predição algorítmica. A Seção 5 desenvolve o debate jurídico sobre a configuração de discriminação abusiva à luz do art. 6º, IX da LGPD, discute a responsabilidade do poder público e apresenta medidas mitigadoras (transparência e auditoria algorítmica, AIPD e atualização das bases de dados) para um uso ético e legal da vigilância algorítmica na segurança pública.

2 FUNDAMENTOS TEÓRICOS DA VIGILÂNCIA E DO CONTROLE SOCIAL

2.1 DO PANÓPTICO DE FOUCAULT À SOCIEDADE DA TRANSPARÊNCIA DE HAN: A EVOLUÇÃO DA VIGILÂNCIA

A vigilância como mecanismo de controle social não é um fenômeno recente. Sua história remonta a práticas longínquas de observação e monitoramento, mas ganhou contornos específicos com o advento da modernidade e a necessidade de gerenciar populações em larga escala. A evolução da vigilância reflete as transformações sociais, políticas e tecnológicas, culminando nas complexas formas digitais contemporâneas. Para compreender essa trajetória, é fundamental revisitar as contribuições de Michel Foucault e Byung-Chul Han, que oferecem lentes distintas, para analisar o poder da observação e do controle.

2.1.1 O panoptismo e a disciplina (Michel Foucault)

Michel Foucault (2021, p. 335-337), em sua obra Microfísica do Poder, introduziu o conceito de panoptismo, inspirado no projeto arquitetônico de Jeremy Bentham. O panóptico é uma estrutura circular com uma torre central de onde um observador pode ver todas as celas dispostas ao redor, sem que os observados saibam se estão sendo vigiados em um dado momento. O poder do panóptico reside não na vigilância constante e efetiva, mas na sensação de ser constantemente vigiado. Essa incerteza induz os indivíduos a internalizarem a norma e a se disciplinarem, agindo como se estivessem sempre sob o olhar dominador e vigilante. Foucault argumentou que o panoptismo transcende a arquitetura prisional, tornando-se um modelo de poder disciplinar que se espalha por diversas instituições sociais, como escolas, hospitais e fábricas, moldando comportamentos e produzindo corpos dóceis e úteis.

No panóptico, a visibilidade é uma armadilha. O indivíduo é visto, mas não vê. É objeto de informação, mas nunca sujeito de comunicação. Essa assimetria de poder garante a eficácia do controle, pois a disciplina opera de forma automática e generalizada.

A vigilância foucaultiana, portanto, não se limita à repressão, mas atua na produção de subjetividades, normalizando condutas e excluindo o que foge ao padrão.

2.1.2 A sociedade da transparência e a vigilância aperspectivista (Byung-Chul Han)

Byung-Chul Han (2017, p. 10), por sua vez, ofereceu uma crítica contemporânea à vigilância, argumentando que a sociedade atual transcendeu o modelo panóptico de Foucault. Em sua obra Sociedade da Transparência, Han descreveu um cenário onde a vigilância não é imposta por uma torre central e oculta, mas é exercida de forma aperspectivista, ou seja, sem um ponto de vista fixo ou um observador definido. Na sociedade da transparência, os indivíduos se expõem voluntariamente, compartilhando dados e informações em plataformas digitais, movidos por um imperativo de visibilidade e conexão.

Para Han (2017, p. 19), a vigilância digital não é coercitiva, mas sedutora. As pessoas se tornam seus próprios vigilantes, produzindo e disponibilizando dados que são, então, coletados e analisados por algoritmos. Essa autoexposição, que se apresenta como liberdade, na verdade, culmina em uma nova forma de controle, mais eficiente e sutil do que a disciplina foucaultiana. A ausência de um inimigo claro ou de uma estrutura de poder visível torna a resistência mais difícil, pois o controle se manifesta como uma escolha individual, uma busca por reconhecimento e pertencimento.

A sociedade da transparência, paradoxalmente, leva ao fim da privacidade, não por

coerção, mas por uma compulsão à exposição que anula a distinção entre o público e o privado. Nesse cenário, os indivíduos, habitantes de um panóptico digital, alimentam voluntariamente o olhar vigilante com informações pessoais, escolhendo, muitas vezes, renunciar sua esfera íntima. Essa entrega, por vezes indiscreta, revela um contexto em que liberdade e controle se tornam indistinguíveis.

2.2 A VIGILÂNCIA ALGORÍTMICA: CONCEITOS E IMPLICAÇÕES NA SOCIEDADE DIGITAL

A vigilância algorítmica representa a convergência das tendências históricas da vigilância com as capacidades computacionais da era digital. Ela se distingue das formas anteriores de monitoramento por sua escala, velocidade e automação do processo de coleta, análise e tomada de decisão. Em sua essência, a vigilância algorítmica é o uso de algoritmos e sistemas de inteligência artificial para monitorar, analisar e, em muitos casos, prever o comportamento de indivíduos e grupos.

2.2.1 Algoritmos, *big data* e predição comportamental

No cerne da vigilância algorítmica estão os algoritmos, sequências de instruções lógicas que permitem a um computador realizar tarefas específicas. Quando aplicados a grandes volumes de dados, conhecidos como *big data*, esses algoritmos podem identificar padrões, correlações e tendências que seriam imperceptíveis à análise humana. O *big data*, segundo Munhoz (2022), é caracterizado pelos 3 Vs: volume (quantidade massiva de dados), velocidade (rapidez na geração e processamento) e variedade (diversidade de formatos e fontes de dados).

A combinação de algoritmos sofisticados e *big data* possibilita a predição comportamental. Isso significa que, a partir da análise de dados históricos e em tempo real, os sistemas podem inferir probabilidades sobre ações futuras de indivíduos. Por exemplo, algoritmos de reconhecimento facial podem prever a probabilidade de uma pessoa ser um foragido da justiça com base em características faciais e comparação com bancos de dados. Essa capacidade preditiva é utilizada em diversas áreas, desde a personalização de anúncios até a segurança pública e a avaliação de riscos (Costa, Kremer, 2022).

No entanto, a predição comportamental não é infalível. Ela se baseia em modelos estatísticos e em dados de treinamento que podem conter vieses inerentes, refletindo desigualdades sociais e preconceitos existentes na sociedade. Se os dados de treinamento são

enviesados, os algoritmos podem replicar e até amplificar esses vieses, levando a decisões discriminatórias.

2.2.2 O poder preditivo e seus riscos sociais

O poder preditivo dos algoritmos, embora prometa eficiência e otimização, acarreta riscos sociais significativos. Um dos principais é a possibilidade de discriminação algorítmica, onde os sistemas produzem resultados desiguais e prejudiciais para determinados grupos de pessoas. Isso pode ocorrer de diversas formas: i) viés nos dados de treinamento, se os dados usados para treinar o algoritmo não são representativos ou contêm preconceitos históricos, o algoritmo aprenderá e reproduzirá esses preconceitos. Por exemplo, sistemas de reconhecimento facial podem ter menor precisão para identificar indivíduos de certas etnias ou gêneros, levando a mais falsos positivos para esses grupos; ii) viés no algoritmo, mesmo com dados de treinamento aparentemente neutros, a forma como o algoritmo é projetado ou os parâmetros que ele prioriza podem introduzir vieses. Por exemplo, um algoritmo pode dar mais peso a certas características que, embora não sejam explicitamente discriminatórias, correlacionam-se com grupos minoritários; iii) impacto desproporcional, ainda que o algoritmo não seja intencionalmente discriminatório, seus resultados podem ter um impacto desproporcional em grupos já marginalizados. Por exemplo, um sistema de predição de criminalidade que foca em áreas de baixa renda pode levar a um policiamento excessivo nessas regiões, aumentando as chances de abordagens e prisões para seus moradores, independentemente de sua real propensão a cometer crimes.

Além da discriminação, o poder preditivo também levanta preocupações sobre a autonomia individual e a liberdade de escolha. Ao prever e, em alguns casos, influenciar o comportamento, os algoritmos podem minar a capacidade dos indivíduos de tomar decisões informadas e de exercer sua autodeterminação.

Outro risco é a opacificação dos processos decisórios. Muitos algoritmos, especialmente os de aprendizado de máquina profundo, operam como caixas pretas, tornando difícil compreender como chegam a determinadas conclusões. Essa falta de transparência dificulta a responsabilização e a contestação de decisões algorítmicas, especialmente quando elas afetam direitos fundamentais.

Em suma, a vigilância algorítmica, com seu poder preditivo, exige uma análise cuidadosa de seus riscos e implicações sociais. A promessa de eficiência e segurança deve ser equilibrada com a proteção dos direitos fundamentais e a garantia de que a tecnologia sirva à

sociedade de forma justa e equitativa.

3 A LEI GERAL DE PROTEÇÃO DE DADOS E OS DIREITOS FUNDAMENTAIS NO CONTEXTO DA VIGILÂNCIA

3.1 A PROTEÇÃO DE DADOS PESSOAIS COMO DIREITO FUNDAMENTAL NO BRASIL (EC Nº 115/2022)

A proteção de dados pessoais, antes tratada de forma esparsa na legislação brasileira, ganhou *status* de direito fundamental com a promulgação da Emenda Constitucional n.º 115, de 10 de fevereiro de 2022. Essa emenda incluiu o inciso LXXIX ao art. 5º da Constituição Federal, estabelecendo que "(...) é assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais" (Brasil, 2022, *s.p.*). Essa alteração constitucional representa um marco significativo, elevando a proteção de dados ao patamar de cláusula pétrea e reforçando a importância da privacidade e da autodeterminação informativa no ordenamento jurídico brasileiro.

Antes da EC n.º 115/2022, a proteção de dados já era inferida de outros direitos fundamentais, como a privacidade, intimidade e honra, previstos no próprio art. 5º da Carta Magna. No entanto, a explicitação desse direito confere maior segurança jurídica e um arcabouço mais robusto para a defesa dos titulares de dados, especialmente diante do cenário de crescente coleta e tratamento de informações pessoais por parte de entidades públicas e privadas. A LGPD, promulgada em 2018, já havia estabelecido as bases para a proteção de dados no país, mas a constitucionalização desse direito reforça sua primazia e a necessidade de que todas as atividades de tratamento de dados estejam em conformidade com os preceitos constitucionais e legais.

3.2 PRINCÍPIOS DA LGPD RELEVANTES PARA A VIGILÂNCIA DIGITAL

A LGPD estabeleceu um conjunto de princípios que devem nortear todas as operações de tratamento de dados pessoais. Esses princípios, elencados no art. 6º da LGPD, são fundamentais para garantir que o tratamento de dados seja realizado de forma ética, transparente e em conformidade com os direitos dos titulares. No contexto da vigilância digital, alguns desses princípios adquirem especial relevância. É o que será tratado a seguir.

3.2.1 Finalidade, adequação e necessidade

Os princípios da finalidade, adequação e necessidade são pilares para o tratamento legítimo de dados pessoais. O princípio da finalidade (art. 6º, I) exige que o tratamento de dados seja realizado para propósitos legítimos, específicos, explícitos e informados ao titular, sem a possibilidade de tratamento posterior de forma incompatível com essas finalidades. Isso significa que a coleta de dados, como no caso da vigilância por reconhecimento facial, deve ter um objetivo claro e previamente definido e não pode ser utilizada para outros fins sem o consentimento do titular ou outra base legal que o justifique.

O princípio da adequação (art. 6º, II) determina que o tratamento de dados deve ser compatível com as finalidades informadas ao titular. Ou seja, os meios utilizados para a vigilância devem ser apropriados para atingir o objetivo proposto. Já o princípio da necessidade (art. 6º, III) impõe que o tratamento de dados deve ser limitado ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação aos objetivos do tratamento. No caso da vigilância por reconhecimento facial, isso implica que apenas os dados estritamente necessários para a identificação e os fins de segurança pública devem ser coletados e processados, evitando a coleta indiscriminada ou excessiva de informações.

3.2.2 Transparência e segurança

Os princípios da transparência (art. 6º, VI) e da segurança (art. 6º, VII) são cruciais para a construção de confiança e para a proteção dos dados pessoais. A transparência exige que o titular tenha acesso claro e preciso às informações sobre o tratamento de seus dados, incluindo a finalidade, a forma e a duração do tratamento, bem como a identificação do controlador. No contexto da vigilância, isso implica que os cidadãos devem ser informados sobre a existência de sistemas de reconhecimento facial, seus objetivos e como seus dados serão utilizados. A falta de transparência pode gerar um ambiente de desconfiança e dificultar o exercício dos direitos dos titulares.

O princípio da segurança demanda que sejam utilizadas medidas técnicas e administrativas aptas a protegerem os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão. Sistemas de vigilância, como o SMART SAMPA, que lidam com dados sensíveis como biometria, devem implementar rigorosas medidas de segurança para evitar vazamentos, fraudes ou usos indevidos

das informações coletadas.

3.2.3 O princípio da não discriminação (art. 6º, IX)

O princípio da não discriminação (art. 6º, IX) é de particular importância para esta pesquisa. Ele estabelece a "(...) impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos" (Brasil, 2018, *s.p.*). Este princípio visa coibir o uso de dados pessoais para gerar ou reforçar preconceitos, estereótipos ou tratamentos desiguais que possam prejudicar indivíduos ou grupos. A discriminação, nesse contexto, não se limita apenas à intenção do agente de tratamento, mas também aos efeitos que o tratamento de dados pode gerar.

No cenário da vigilância algorítmica, a discriminação pode se manifestar de forma sutil e não intencional, muitas vezes decorrente de vieses presentes nos dados de treinamento dos algoritmos ou na própria concepção do sistema. No contexto do reconhecimento facial, tais algoritmos podem apresentar menor precisão para identificar pessoas de determinadas etnias, gêneros ou idades, levando a uma maior incidência de falsos positivos para esses grupos. Quando esses falsos positivos resultam em abordagens policiais indevidas, constrangimentos ou restrições de liberdade, configura-se um tratamento de dados com fins discriminatórios abusivos, mesmo que não haja uma intenção explícita de discriminar.

A LGPD, ao incluir expressamente o princípio da não discriminação, busca proteger os titulares de dados contra esses efeitos adversos do tratamento automatizado. A análise de um sistema como o SMART SAMPA sob a ótica desse princípio exige a verificação não apenas da legalidade formal do tratamento, mas também de seus impactos concretos na vida dos indivíduos, especialmente daqueles que podem ser desproporcionalmente afetados por vieses algorítmicos.

3.3 DADOS PESSOAIS SENSÍVEIS E DADOS BIOMÉTRICOS NA LGPD

A LGPD confere proteção especial aos dados pessoais sensíveis, definidos no art. 5º, inciso II, como aqueles que revelam origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural. O tratamento de dados sensíveis é, em regra, proibido, salvo exceções específicas previstas no art. 11 da LGPD (Brasil, 2018, *s.p.*).

Os dados biométricos, que incluem características físicas ou comportamentais únicas de um indivíduo, como impressões digitais, íris, voz e, crucialmente para esta pesquisa, a face, são considerados dados pessoais sensíveis. Isso se deve ao seu alto potencial de identificação e à irreversibilidade de sua coleta, o que os torna particularmente vulneráveis a usos indevidos e a riscos de discriminação. O reconhecimento facial, ao coletar e processar dados biométricos, está sujeito às regras mais rigorosas da LGPD para dados sensíveis.

O tratamento de dados biométricos para fins de segurança pública, embora possa ser justificado pelo legítimo interesse do Estado, deve observar rigorosamente os princípios da LGPD, especialmente a necessidade e a proporcionalidade. A coleta e o uso desses dados devem ser estritamente limitados aos fins específicos e legítimos, e qualquer desvio que resulte em discriminação ou violação de direitos é expressamente vedado pelo art. 6º, IX.

3.4 EXCEÇÃO DE SEGURANÇA PÚBLICA E ALCANCE PRINCIPIOLÓGICO

Ainda que o art. 4º, III da LGPD preveja a exclusão de seu âmbito de aplicação para o tratamento de dados pessoais realizado para fins exclusivamente ligados à segurança pública, essa exceção não se estende aos princípios constitucionais de proteção de dados pessoais, introduzidos no ordenamento jurídico brasileiro pela Emenda Constitucional n.º 115/2022 (art. 5º, LXXIX da CF/1988) (Brasil, 2022, *s.p.*). Tais princípios, alicerçados na dignidade da pessoa humana, na autodeterminação informativa e na não discriminação, mantêm plena aplicabilidade às atividades de vigilância estatal.

A exclusão prevista no art. 4º da LGPD deve, portanto, ser interpretada de forma restritiva. O poder público, mesmo em ações voltadas à segurança, permanece obrigado a adotar parâmetros de proporcionalidade, necessidade e minimização dos dados, bem como a evitar qualquer forma de tratamento discriminatório ilícito ou abusivo. A ausência de vinculação direta ao regime jurídico da LGPD não autoriza práticas que possam produzir resultados desproporcionais, tampouco exime o Estado de implementar avaliações de impacto e mecanismos de controle (*accountability*), com vistas a assegurar a legalidade, a transparência e a proteção dos direitos fundamentais dos indivíduos.

3.5 O PAPEL DA AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD) NA FISCALIZAÇÃO DA VIGILÂNCIA

A Autoridade Nacional de Proteção de Dados (ANPD) é o órgão responsável por zelar

pela proteção de dados pessoais e por fiscalizar o cumprimento da LGPD no Brasil. Criada pela própria lei protetiva de dados, a ANPD possui competências ampla, incluindo a edição de normas e regulamentos, a fiscalização e aplicação de sanções, a promoção do conhecimento sobre proteção de dados e a cooperação com outras autoridades.

No contexto da vigilância digital, a ANPD desempenha um papel fundamental. Cabe à Autoridade Nacional, inclusive no uso de reconhecimento facial por parte do poder público:

1. Fiscalizar se os sistemas de vigilância, como o SMART SAMPA, estão em conformidade com a LGPD, observando os princípios, as bases legais e as medidas de segurança;
2. Regulamentar aspectos específicos do tratamento de dados biométricos e do uso de inteligência artificial, estabelecendo diretrizes para mitigar riscos de discriminação e vieses algorítmicos;
3. Receber denúncias de titulares de dados sobre violações de seus direitos e investigar possíveis irregularidades no tratamento de dados por sistemas de vigilância;
4. Aplicar sanções em caso de descumprimento da LGPD, que podem variar de advertências a multas e bloqueio de dados; e
5. Promover a conscientização sobre os riscos e direitos relacionados ao uso de tecnologias de vigilância, incentivando a transparência e o controle social.

A atuação da ANPD é essencial para garantir que a implementação de tecnologias de vigilância na segurança pública seja realizada de forma responsável, respeitando os direitos fundamentais dos cidadãos e evitando que a busca por segurança se traduza em um cenário de vigilância indiscriminada e discriminatória.

4 O SISTEMA SMART SAMPA: OPERAÇÃO, INCONSISTÊNCIAS E POTENCIAL DISCRIMINATÓRIO

4.1 APRESENTAÇÃO DO PROGRAMA SMART SAMPA: OBJETIVOS E FUNCIONAMENTO

Na sociedade contemporânea, diante de um cenário marcado pela violência, pelos elevados índices de criminalidade e por um sentimento generalizado de insegurança, observa-se o empenho do poder público na adoção de tecnologias emergentes voltadas à otimização da segurança pública. Nesse contexto, destaca-se a crescente adoção de sistemas autônomos de reconhecimento facial, por meio dos quais o Estado busca concretizar os deveres que lhe são

atribuídos, valendo-se dos avanços tecnológicos como instrumentos de gestão e controle social (Melo, 2020).

Um exemplo emblemático dessa tendência é o Programa SMART SAMPA, implementado pela Prefeitura de São Paulo. A iniciativa visa integrar tecnologias de vigilância de última geração no combate à criminalidade e na promoção da segurança urbana. Seu principal eixo é o uso do reconhecimento facial automatizado, operacionalizado por meio de uma rede de câmeras estrategicamente posicionadas em áreas de grande circulação. Esses dispositivos têm como finalidade a identificação de indivíduos com mandados de prisão em aberto ou que estejam sob investigação criminal.

O programa declara como objetivos centrais o aumento da eficiência das forças de segurança, a agilização na identificação de foragidos e a contribuição para a redução dos índices de criminalidade na capital paulista (São Paulo, 2025).

O funcionamento do SMART SAMPA está baseado na captura de imagens faciais em tempo real pelas câmeras de vigilância. Essas imagens são, então, processadas por algoritmos de inteligência artificial que as comparam com um banco de dados de indivíduos procurados, alimentado principalmente pelo BNMP e outras bases de dados criminais. Em caso de alta similaridade entre uma face capturada e uma face no banco de dados, um alerta é gerado e transmitido às equipes de campo, que procedem à abordagem e verificação da identidade do indivíduo (São Paulo, 2025).

O programa também se propõe a auxiliar em outras frentes, como a localização de pessoas desaparecidas e o apoio a programas de proteção a vítimas de violência – como o Guardiã Maria da Penha –, além de cooperar com investigações da Polícia Civil, fornecendo imagens e informações relevantes (São Paulo, 2025). A promessa é de uma cidade mais segura e monitorada, onde a tecnologia atua como um braço auxiliar na manutenção da ordem pública.

4.2 ANÁLISE DAS INCONSISTÊNCIAS OPERACIONAIS DO SMART SAMPA

Apesar dos objetivos declarados de eficiência e segurança, o Relatório de Transparência do Programa SMART SAMPA, referente ao período de 21 de novembro de 2024 a 21 de maio de 2025, revela uma série de inconsistências operacionais que merecem atenção crítica. O relatório detalha os resultados das abordagens realizadas, expondo as razões pelas quais um número significativo de pessoas, inicialmente identificadas pelo sistema, não foi efetivamente presa ou foi liberada após condução à delegacia (São Paulo, 2025).

Durante o período analisado, foram realizadas 1.246 abordagens, resultando em 1.153

prisões. No entanto, o relatório aponta que **23 pessoas foram conduzidas à delegacia por inconsistência no reconhecimento facial** e, após verificação formal, constatou-se não haver pendências. Além disso, outras 11 pessoas foram conduzidas e liberadas por inconsistência cadastral e 20 por falta de baixa do mandado no BNMP (São Paulo, 2025). Esses dados são cruciais para entender as falhas do sistema.

As principais inconsistências identificadas no relatório são:

4.2.1 Falta de baixa de mandado no BNMP

O relatório indica que 20 pessoas foram conduzidas à delegacia e, posteriormente, foram liberadas devido à falta de baixa do mandado no BNMP (São Paulo, 2025). Isso significa que, embora houvesse um mandado de prisão registrado no sistema, este já havia sido cumprido ou revogado, mas a informação não havia sido devidamente atualizada no BNMP. Essa falha, que não é diretamente do sistema de reconhecimento facial, mas da base de dados alimentadora, resulta em abordagens indevidas e privação temporária da liberdade de indivíduos que já não possuíam pendências judiciais. A responsabilidade pela atualização do BNMP recai sobre as autoridades judiciárias e policiais, mas a utilização de uma base de dados desatualizada pelo SMART SAMPA gera consequências diretas para os cidadãos.

4.2.2 Inconsistência cadastral

Outras 11 pessoas foram conduzidas e liberadas por inconsistência cadastral (São Paulo, 2025). Essa categoria abrange situações em que os dados do indivíduo no banco de dados não correspondiam à sua identidade real ou estavam desatualizados. Erros de digitação, homônimos ou informações incompletas podem levar o sistema a gerar um alerta para a pessoa errada. Assim como a falta de baixa no BNMP, a inconsistência cadastral aponta para a fragilidade das bases de dados utilizadas pelo sistema, que, se não forem precisas e constantemente atualizadas, podem levar a abordagens equivocadas e constrangimentos desnecessários.

4.2.3 Inconsistência no reconhecimento facial (falsos positivos e conduções indevidas)

Entre as inconsistências operacionais do SMART SAMPA, a falha mais crítica está diretamente associada ao módulo de reconhecimento facial automatizado. De acordo com o

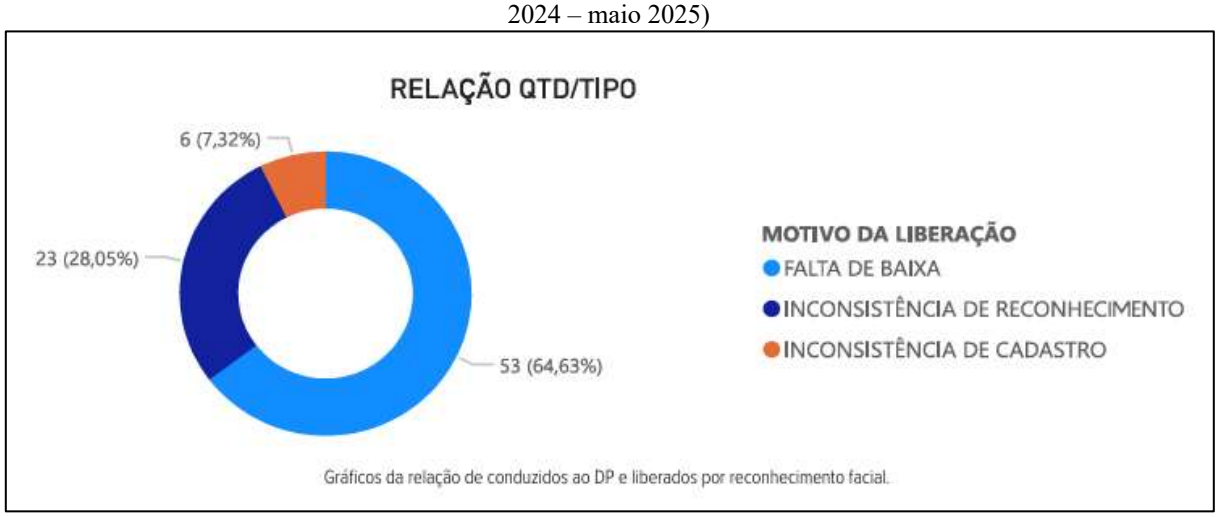
Relatório de Transparência (São Paulo, 2025), no período de novembro de 2024 a maio de 2025, 82 (oitenta e duas) pessoas foram abordadas e conduzidas ao Distrito Policial, sendo posteriormente liberadas por ausência de confirmação de pendências judiciais.

Dentre esse total, os dados se distribuem da seguinte forma:

- 53 casos decorreram de falta de baixa de mandado no Banco Nacional de Mandados de Prisão (BNMP);
- 6 casos tiveram origem em inconsistências cadastrais, atribuídas a erros ou desatualização das bases de dados integradas;
- 23 situações resultaram de falsos positivos gerados pelo reconhecimento facial, representando 28,05% das ocorrências.

O relatório destaca que, nesses 23 casos, a semelhança facial detectada pelo sistema (em situações como presença de gêmeos idênticos, baixa qualidade das imagens capturadas ou alterações na aparência do indivíduo) exigiu verificação formal pela autoridade policial para afastar qualquer pendência. Tais falsos positivos evidenciam a limitação técnica do algoritmo e o risco de constrangimentos indevidos a cidadãos inocentes.

Imagem 1: Distribuição percentual das abordagens liberadas por inconsistências no SMART SAMPA (nov. 2024 – maio 2025)



Fonte: São Paulo, 2025

O fenômeno dos falsos positivos, por sua natureza, configura uma falha grave no tratamento de dados biométricos, pois atinge diretamente direitos fundamentais, como a liberdade de locomoção, a presunção de inocência e a dignidade da pessoa humana. A situação de condução indevida, ainda que temporária, caracteriza um constrangimento público e um ônus desproporcional, sendo juridicamente irrelevante a ausência de dolo por parte do controlador público. As razões para esses erros podem ser diversas, incluindo:

1. Baixa qualidade da imagem: Condições de iluminação, ângulo da câmera, obstáculos (chapéus, óculos, máscaras) podem comprometer a qualidade da imagem capturada, dificultando a análise precisa pelo algoritmo;

2. Similaridade facial: Pessoas com características faciais muito semelhantes (como gêmeos idênticos) podem ser confundidas pelo sistema;

3. Variações na aparência: Mudanças na aparência do indivíduo ao longo do tempo (envelhecimento, barba, cabelo) podem afetar a precisão do reconhecimento; e

4. Viés algorítmico: Conforme evidenciado na revisão teórica, algoritmos de reconhecimento facial podem apresentar vieses inerentes, com menor precisão para identificarem corretamente indivíduos de certas etnias, gêneros ou idades. Isso pode levar a uma maior incidência de falsos positivos para esses grupos, que são desproporcionalmente abordados e submetidos a verificações.

Esses 23 registros (28,05 % das conduções analisadas) transcendem meras falhas técnicas, evidenciando fragilidade estrutural do modelo de vigilância algorítmica empregado pelo SMART SAMPA (Relatório de Transparência, 2025). O art. 6º, IX, da LGPD veda o tratamento de dados para fins discriminatórios ilícitos ou abusivos, alcançando igualmente os efeitos indiretos decorrentes de vieses tecnológicos. A condução de pessoas inocentes, submetidas a constrangimento público, privação temporária de liberdade e verificações desnecessárias, revela violação a direitos fundamentais, como a dignidade da pessoa humana e presunção de inocência, e põe em xeque a proporcionalidade e a legitimidade do reconhecimento facial quando seus erros recaem sobre indivíduos sem qualquer vínculo com ilícitos.

4.3 A PREDIÇÃO ALGORÍTMICA NO SMART SAMPA E A GERAÇÃO DE FALSOS POSITIVOS

O sistema SMART SAMPA opera com base em um modelo de predição algorítmica. Ele não apenas compara imagens, mas utiliza algoritmos para inferir a probabilidade de uma pessoa ser um foragido da justiça. Essa predição é feita a partir de um conjunto de dados de treinamento e de parâmetros definidos pelos desenvolvedores do sistema. Quando o algoritmo calcula uma alta probabilidade de correspondência, mesmo que não seja uma certeza, um alerta é gerado, levando à abordagem policial.

A geração de falsos positivos é uma consequência direta da natureza probabilística da predição algorítmica. Nenhum algoritmo é 100% preciso e sempre haverá uma margem de erro.

No contexto do reconhecimento facial para segurança pública, essa margem de erro tem implicações severas. Um falso positivo não é apenas um erro técnico; é uma pessoa inocente que é erroneamente identificada como criminosa, resultando em uma abordagem policial e, como visto no relatório do SMART SAMPA, na condução à delegacia.

O problema se agrava quando os vieses algorítmicos entram em jogo. Se o algoritmo foi treinado predominantemente com dados de um determinado grupo demográfico, sua precisão pode ser significativamente menor para outros grupos. Estudos demonstram que sistemas de reconhecimento facial comerciais têm desempenho muito pior para identificar pessoas pretas, especialmente na identificação de mulheres de pele escura, aumentando a probabilidade de falsos positivos para esses segmentos da população (Santos, Costa, David, Pedro, 2023). Isso significa que a predição algorítmica, ao invés de ser neutra, pode perpetuar e amplificar desigualdades sociais e raciais existentes, tornando certos grupos mais suscetíveis a serem erroneamente identificados e abordados.

4.4 A DISCRIMINAÇÃO ABUSIVA NO CONTEXTO DO SMART SAMPA

A análise das inconsistências do SMART SAMPA, em particular os 23 casos de condução indevida por erro de reconhecimento facial, levanta a séria questão da discriminação abusiva. Embora o relatório não forneça dados qualitativos ou quantitativos sobre o perfil demográfico das pessoas erroneamente identificadas, a literatura sobre vieses algorítmicos sugere que esses erros não são distribuídos aleatoriamente na população (Santos, Costa, David, Pedro, 2023).

4.4.1 Impacto nos direitos fundamentais dos indivíduos abordados indevidamente

Para as 23 pessoas conduzidas à delegacia por inconsistência no reconhecimento facial, o impacto em seus direitos fundamentais é inegável. A abordagem policial baseada em um erro do sistema, seguida da condução a uma delegacia, mesmo que, para posterior liberação, configura uma violação de diversos direitos:

1. Liberdade de locomoção: A pessoa é impedida de seguir seu caminho, sendo detida e levada contra sua vontade para um ambiente policial;
2. Dignidade da pessoa humana: A situação de ser erroneamente identificado como criminoso e abordado publicamente gera constrangimento, humilhação e estigmatização, ferindo a dignidade do indivíduo;

3. Presunção de inocência: A abordagem e condução, mesmo que para averiguação, colocam o indivíduo sob suspeita sem justa causa, contrariando o princípio da presunção de inocência; e

4. Privacidade e proteção de dados: Os dados biométricos da pessoa foram coletados e processados, resultando em um erro que a expôs a uma situação vexatória. Isso levanta questões sobre a adequação e a necessidade do tratamento desses dados, bem como a segurança do sistema.

Esses impactos são ainda mais graves quando se considera que a abordagem é automatizada, baseada em uma predição algorítmica falha, e não em uma suspeita concreta e individualizada. A pessoa se torna um alvo de um sistema que, por suas falhas, trata-a como potencial criminosa, mesmo sendo inocente.

4.4.2 Discussão sobre o viés algorítmico e a potencial discriminação racial/social

A ausência de dados demográficos no relatório do SMART SAMPA impede uma análise quantitativa direta sobre a existência de discriminação racial ou social nos casos de falsos positivos. No entanto, a vasta literatura sobre o tema, incluindo o artigo As máquinas podem ser racistas? Como evitar a discriminação algorítmica (Yoshida, 2022), aponta para a alta probabilidade de que os vieses algorítmicos resultem em discriminação. Como dito, sistemas de reconhecimento facial, em geral, demonstram menor precisão para identificarem corretamente indivíduos de grupos minoritários, como pessoas negras e mulheres, o que os torna mais propensos a serem falsamente identificados (Santos, Costa, David, Pedro, 2023).

Se essa tendência é replicada no SMART SAMPA, os 23 casos de condução indevida por erro de reconhecimento facial podem não terem sido aleatórios, mas sim um reflexo de um viés sistêmico. Isso significaria que pessoas negras, por exemplo, teriam uma probabilidade maior de serem erroneamente identificadas e abordadas, configurando uma discriminação indireta, mas com efeitos concretos e abusivos. Essa discriminação é abusiva, porque decorre de um tratamento de dados que, embora não intencional, gera um impacto desproporcional e prejudicial a um grupo específico, violando o art. 6º, IX da LGPD.

A discussão sobre o viés algorítmico é fundamental para compreender como a tecnologia, que é apresentada como neutra e objetiva, pode, na verdade, reproduzir e intensificar desigualdades sociais. A falta de transparência sobre os dados de treinamento dos algoritmos e sobre as métricas de desempenho para diferentes grupos demográficos dificulta a auditoria e a responsabilização, tornando o problema da discriminação algorítmica ainda mais complexo.

5 DEBATE JURÍDICO: A VIOLAÇÃO DO ART. 6º, IX DA LGPD PELAS PRÁTICAS DO SMART SAMPA

5.1 ARGUMENTOS JURÍDICOS PARA A CARACTERIZAÇÃO DA DISCRIMINAÇÃO ABUSIVA

A análise das inconsistências operacionais do sistema SMART SAMPA, particularmente os 23 casos de condução indevida à delegacia por erro de reconhecimento facial, fornece subsídios robustos para argumentar que as práticas do programa podem configurar uma violação ao art. 6º, inciso IX da LGPD, que veda o tratamento de dados para fins discriminatórios ilícitos ou abusivos. A caracterização dessa discriminação não se baseia necessariamente em uma intenção deliberada de discriminar, mas nos efeitos concretos e desproporcionais que o tratamento de dados gera.

Primeiro, é fundamental reiterar que o reconhecimento facial envolve o tratamento de dados biométricos, que são classificados pela LGPD como dados pessoais sensíveis (art. 5º, II). O tratamento de dados sensíveis possui regras mais rigorosas e, em regra, é proibido, salvo exceções específicas (art. 11). Embora o uso para segurança pública possa ser enquadrado em bases legais como o cumprimento de obrigação legal ou a execução de políticas públicas (art. 7º, III e art. 11, II, d), isso não exime o controlador de observar os princípios da lei, especialmente o da não discriminação.

O art. 6º, IX, da LGPD, ao proibir o tratamento para fins discriminatórios ilícitos ou abusivos, abrange tanto a discriminação direta (intencional) quanto a indireta (por efeito). No caso do SMART SAMPA, a discriminação se manifesta de forma indireta e abusiva. É indireta porque não há uma declaração explícita de que o sistema visa discriminar. No entanto, é abusiva porque, ao gerar falsos positivos que resultam em abordagens e conduções indevidas de pessoas inocentes, o sistema impõe um ônus desproporcional e prejudicial a esses indivíduos. A abusividade reside no fato de que o tratamento de dados, embora possa ter uma finalidade legítima (segurança pública), excede os limites da razoabilidade e da proporcionalidade ao produzir efeitos lesivos e injustos (Doneda, 2019).

Os 23 casos de condução indevida por inconsistência no reconhecimento facial são a prova cabal dessa abusividade. Essas pessoas foram submetidas a uma privação de liberdade, constrangimento público e estigmatização, sem que houvesse qualquer ilícito de sua parte. O erro do algoritmo, que se traduziu em um falso positivo, não é um mero erro técnico; é um erro

com consequências reais e negativas para a vida dos cidadãos. Quando esses erros são sistemáticos e afetam desproporcionalmente determinados grupos a discriminação abusiva se torna ainda mais evidente.

Além disso, a violação dos princípios da necessidade e da adequação (art. 6º, III e II) também contribui para a caracterização da discriminação abusiva. Se o sistema gera um número significativo de falsos positivos, questiona-se se ele é realmente adequado para a finalidade de identificar criminosos de forma precisa e se o tratamento de dados biométricos é estritamente necessário na forma como está sendo realizado, dado o alto risco de erro e o impacto nos direitos fundamentais. A LGPD exige que o tratamento seja limitado ao mínimo necessário e que os dados sejam pertinentes e proporcionais à finalidade. Abordar e conduzir inocentes não é um resultado proporcional ou necessário para a finalidade de prender foragidos.

5.2 A RESPONSABILIDADE DO PODER PÚBLICO E DOS AGENTES DE TRATAMENTO DE DADOS

A LGPD estabelece a responsabilidade dos agentes de tratamento de dados, que incluem o controlador (quem toma as decisões sobre o tratamento) e o operador (quem realiza o tratamento em nome do controlador). No caso do SMART SAMPA, o Poder Público (Prefeitura de São Paulo e órgãos de segurança) atua como controlador, sendo o principal responsável por garantir a conformidade com a LGPD e pelos danos causados pelo tratamento de dados (Brasil, 2018, *s.p.*).

O art. 42 da LGPD prevê a responsabilidade civil dos agentes de tratamento por danos patrimoniais, morais, individuais ou coletivos, causados por violação à legislação de proteção de dados pessoais. No caso das 23 pessoas conduzidas indevidamente, há um claro dano moral e, potencialmente, material (por exemplo, perda de dia de trabalho). O Poder Público, como controlador, tem o dever de indenizar esses danos, independentemente de culpa, uma vez que a responsabilidade é objetiva em casos de violação da LGPD (Brasil, 2018, *s.p.*).

Além disso, a responsabilidade objetiva do Estado encontra respaldo no art. 37, §6º da Constituição Federal, que consagra a teoria do risco administrativo para atos da Administração Pública, e é reforçada pelo art. 927, parágrafo único do Código Civil, que impõe responsabilidade objetiva para atividades que envolvem risco acentuado a terceiros, como é o caso do tratamento automatizado de dados biométricos.

É fundamental ressaltar que a responsabilidade do Estado por atos que geram dano moral em abordagens policiais indevidas é um entendimento consolidado na jurisprudência do

Superior Tribunal de Justiça (STJ). O STJ tem reiteradamente afirmado que a abordagem policial realizada com excesso, mesmo que não resulte em prisão ou condenação, configura abuso de autoridade e gera dano moral. Para a Corte, a comprovação do prejuízo concreto é dispensável, pois os transtornos, a dor, o sofrimento, o constrangimento e o vexame experimentados pela vítima são inerentes ao próprio fato. A simples submissão a uma situação vexatória e humilhante, decorrente de uma ação estatal desproporcional ou equivocada, é suficiente para caracterizar o dano moral indenizável (STJ, 2011).

Essa compreensão do STJ é de extrema relevância para o caso do SMART SAMPA. As 23 conduções indevidas, motivadas por falhas no reconhecimento facial, expuseram cidadãos inocentes a um constrangimento público e a uma privação de liberdade temporária, configurando um dano moral *in re ipsa*, ou seja, que decorre do próprio fato. A tecnologia, ao invés de ser uma ferramenta neutra, tornou-se o instrumento de um abuso que, embora algorítmico em sua origem, possui consequências humanas diretas e severas. A responsabilidade do Poder Público, neste cenário, é inafastável.

Isso porque a responsabilidade objetiva do controlador público está amparada por três pilares normativos: (i) o art. 37, §6º da Constituição Federal, que consagra a teoria do risco administrativo para atos da Administração; (ii) o art. 42 da LGPD, que impõe responsabilidade civil independentemente de culpa pelos danos decorrentes do tratamento de dados pessoais; e (iii) o art. 927, parágrafo único do Código Civil, que prevê responsabilidade objetiva para atividades que impliquem risco elevado, como o uso de algoritmos e bases de dados biométricas suscetíveis a falsos positivos.

Além da responsabilidade civil, o Poder Público está sujeito à fiscalização e às sanções administrativas da Autoridade Nacional de Proteção de Dados (ANPD). A ANPD pode aplicar advertências, multas (simples ou diárias), publicização da infração, bloqueio ou eliminação dos dados pessoais a que se refere a infração, entre outras medidas (art. 52 da LGPD). A ocorrência de falsos positivos e a potencial discriminação algorítmica são elementos que a ANPD deve considerar em sua atuação fiscalizatória, podendo exigir a revisão dos procedimentos, a auditoria dos algoritmos e a implementação de medidas corretivas.

É crucial que o Poder Público não se exima de sua responsabilidade alegando a natureza técnica do sistema ou a ausência de intenção discriminatória. A LGPD foca nos efeitos do tratamento de dados. Se o sistema, por suas falhas e vieses, produz resultados discriminatórios e abusivos, a responsabilidade do controlador é inafastável. Isso implica o dever de investigar as causas dos falsos positivos, especialmente se há um padrão que indique viés algorítmico, e de adotar medidas efetivas para mitigar esses riscos.

5.3 MEDIDAS MITIGADORAS E A NECESSIDADE DE TRANSPARÊNCIA E AUDITORIA ALGORÍTMICA

Para mitigar os riscos de discriminação abusiva e garantir a conformidade com a LGPD, o sistema SMART SAMPA e outras iniciativas de vigilância algorítmica precisam adotar uma série de medidas. O próprio relatório de transparência do SMART SAMPA menciona algumas ações de aprimoramento, como o aumento da similaridade e a verificação humana (São Paulo, 2025). No entanto, essas medidas podem não ser suficientes para endereçarem o problema do viés algorítmico e da discriminação indireta.

É imperativa a transparência algorítmica. Isso significa que o Poder Público deve divulgar informações detalhadas sobre como os algoritmos de reconhecimento facial são desenvolvidos, quais dados são utilizados para treinamento, quais são as métricas de desempenho (incluindo taxas de falsos positivos e falsos negativos para diferentes grupos demográficos) e como as decisões são tomadas pelo sistema. A opacidade dos algoritmos, que operam como caixas pretas, impede a fiscalização e a responsabilização efetiva (Santos, Costa, David, Pedro, 2023). A transparência permite que a sociedade civil, pesquisadores e órgãos de controle avaliem a justiça e a equidade do sistema.

Associada à transparência, a auditoria algorítmica é essencial. Auditorias independentes devem ser realizadas para identificarem e corrigirem vieses nos algoritmos e nos dados de treinamento. Essas auditorias devem ser contínuas e incluir testes rigorosos para avaliar o desempenho do sistema em diferentes grupos populacionais, buscando garantir que a precisão seja equitativa e que não haja impactos desproporcionais. A auditoria deve ser capaz de identificar se, por exemplo, pessoas negras ou mulheres são mais propensas a serem falsamente identificadas e propor soluções para corrigir essas disparidades (Yoshida, 2022).

Outras medidas mitigadoras incluem:

1. Revisão e atualização constante das bases de dados: As inconsistências relacionadas à falta de baixa de mandados no BNMP e a dados cadastrais desatualizados demonstram a necessidade de um processo rigoroso de validação e atualização das informações que alimentam o sistema;

2. Verificação humana robusta: Embora o relatório mencione a verificação humana, é preciso garantir que essa etapa seja realmente eficaz e que os operadores estejam capacitados para identificarem e corrigirem erros do sistema, evitando a condução indevida de inocentes. A decisão final sobre a abordagem e condução deve sempre ser humana e baseada

em elementos concretos, e não apenas na predição algorítmica;

3. Mecanismos de responsabilização e reparação: É fundamental que existam canais claros e acessíveis para que os indivíduos que forem vítimas de falsos positivos possam apresentar denúncias, ter seus casos investigados e receber a devida reparação pelos danos sofridos; e

4. Avaliação de Impacto à Proteção de Dados (AIPD): A LGPD prevê a realização de AIPD para operações de tratamento de dados que possam gerar riscos aos direitos e liberdades civis dos titulares (art. 38). O uso de reconhecimento facial para segurança pública é um caso clássico que exige uma AIPD rigorosa, que deve ser pública e incluir a análise dos riscos de discriminação.

5.4 PROPOSTAS PARA UM USO ÉTICO E LEGAL DA VIGILÂNCIA ALGORÍTMICA NA SEGURANÇA PÚBLICA

Para que a vigilância algorítmica na segurança pública seja ética e legal, é necessário ir além da mera conformidade formal com a LGPD e buscar um equilíbrio entre a segurança e os direitos fundamentais. Algumas propostas incluem:

1. Moratória ou banimento de tecnologias de reconhecimento facial em espaços públicos: Diante dos riscos comprovados de vieses e discriminação, bem como da dificuldade de controle e responsabilização, alguns especialistas e organizações da sociedade civil defendem uma moratória ou, até mesmo, o banimento do uso de reconhecimento facial em espaços públicos, especialmente para fins de segurança, até que marcos regulatórios mais robustos e tecnologias mais justas sejam desenvolvidos (China's, 2019, *s.p.*);

2. Regulamentação específica para IA na segurança pública: A LGPD oferece um arcabouço geral, mas é necessária uma regulamentação mais específica para o uso de inteligência artificial em áreas sensíveis, como a segurança pública, que aborde questões como vieses algorítmicos, transparência, auditabilidade e a proibição de usos que violem direitos fundamentais;

3. Desenvolvimento de algoritmos justos e equitativos: Investimento em pesquisa e desenvolvimento de algoritmos que sejam projetados desde o início para serem justos e equitativos, com mecanismos de detecção e mitigação de vieses incorporados. Isso inclui a utilização de dados de treinamento diversos e representativos, bem como a aplicação de testes de equidade rigorosos;

4. Participação social e controle democrático: A implementação de sistemas de

vigilância deve ser precedida de amplo debate público e participação social. A sociedade civil, os especialistas e os grupos afetados devem ter voz na definição das políticas de uso dessas tecnologias, garantindo que elas servirão ao interesse público e não se tornem ferramentas de controle e opressão; e

5. Educação e conscientização: Promover a educação e a conscientização sobre os riscos e benefícios da inteligência artificial e da vigilância digital, capacitando os cidadãos a compreenderem seus direitos e a exigirem a responsabilização dos agentes de tratamento.

Em última análise, o uso ético e legal da vigilância algorítmica na segurança pública exige uma mudança de paradigma, onde a tecnologia é vista como uma ferramenta a serviço da sociedade, e não como um fim em si mesma. A segurança não pode vir à custa da liberdade e da dignidade dos cidadãos. A LGPD, com seu princípio da não discriminação, oferece um caminho fundamental para garantir esse equilíbrio.

6 CONSIDERAÇÕES FINAIS

Este artigo buscou analisar a relação entre a vigilância algorítmica implementada pelo sistema SMART SAMPA e a ocorrência de discriminação abusiva à luz do princípio da não discriminação estabelecido no art. 6º, inciso IX da LGPD. A pesquisa demonstrou que, embora a vigilância seja um fenômeno histórico que evoluiu do panóptico de Foucault para a sociedade da transparência de Han, a vigilância algorítmica contemporânea, impulsionada pelo *big data* e pelos algoritmos preditivos, apresenta riscos sociais e jurídicos sem precedentes, especialmente no que tange à discriminação.

Foi evidenciado que a proteção de dados pessoais é um direito fundamental no Brasil, reforçado pela Emenda Constitucional n.º 115/2022 e que a LGPD estabelece princípios basilares para o tratamento de dados, como finalidade, adequação, necessidade, transparência e segurança. O princípio da não discriminação (art. 6º, IX) emergiu como sendo crucial, vedando o tratamento de dados para fins discriminatórios ilícitos ou abusivos, o que abrange a discriminação por efeito, mesmo sem intenção deliberada.

A análise do sistema SMART SAMPA, com base em seu relatório de transparência, revelou inconsistências operacionais significativas, como a falta de baixa de mandados no BNMP, inconsistências cadastrais e, mais criticamente, a ocorrência de 23 casos de condução indevida à delegacia por erro de reconhecimento facial (falsos positivos). Esses falsos positivos, inerentes à natureza probabilística da predição algorítmica, têm um custo humano elevado, violando direitos fundamentais como a liberdade de locomoção, a dignidade da pessoa humana

e a presunção de inocência.

Argumentou-se que esses casos de condução indevida, especialmente se houver um viés algorítmico que afete desproporcionalmente determinados grupos, configuram um tratamento de dados com fins discriminatórios abusivos, em clara violação ao art. 6º, IX da LGPD. A responsabilidade do Poder Público, como controlador dos dados, é objetiva e exige a reparação dos danos e a adoção de medidas corretivas. A opacidade dos algoritmos e a falta de dados demográficos sobre os falsos positivos dificultam a auditoria e a responsabilização, mas não eximem o Estado de sua obrigação de garantir a não discriminação.

Por derradeiro, este estudo contribui para o debate sobre o uso de tecnologias de reconhecimento facial na segurança pública sob diversas perspectivas:

1. Jurídica: Aprofunda a interpretação do princípio da não discriminação da LGPD (art. 6º, IX) no contexto da vigilância algorítmica, demonstrando como os falsos positivos podem configurar discriminação abusiva, mesmo sem intenção discriminatória. Reforça a responsabilidade do Poder Público e a necessidade de fiscalização da ANPD;
2. Social: Evidencia o custo humano e os impactos nos direitos fundamentais de cidadãos inocentes submetidos a abordagens e conduções indevidas por falhas tecnológicas, chamando atenção para a necessidade de um olhar mais crítico sobre a promessa de segurança oferecida por essas tecnologias;
3. Tecnológica: Sublinha a importância da transparência e da auditoria algorítmica para identificar e mitigar vieses, promovendo o desenvolvimento e uso de algoritmos mais justos e equitativos; e
4. Política pública: Oferece subsídios para a formulação de políticas públicas mais responsáveis e éticas no uso da inteligência artificial na segurança, sugerindo medidas como a moratória, regulamentação específica e participação social.

REFERÊNCIAS

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 dispor sobre a competência da União para legislar sobre proteção e tratamento de dados pessoais. Brasília, DF: Presidência da República, [2022]. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/Emendas/Emc/emc115.htm. Acesso em: 27 jul. 2025.

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].

CHINA'S algorithms of repression: reverse engineering a Xinjiang police database. **Human Rights Watch**, Nova York, 1 maio 2019. Disponível em: https://www.hrw.org/report/2019/05/01/chinas-algorithms-repression/reverse engineering-xinjiang-police-database. Acesso em: 24 jul. 2025.

COSTA, Ramon; KREMER, Bianca. Inteligência artificial e discriminação: desafios e perspectivas para a proteção de grupos vulneráveis diante das tecnologias de reconhecimento facial. **Direitos Fundamentais & Justiça**, Belo Horizonte, ano 16, número especial, p. 145-167, out. 2022. Disponível em: https://dfj.emnuvens.com.br/dfj/article/view/1316/1065. Acesso em: 24 jul. 2025.

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. Rio de Janeiro: Renovar, 2019.

FOUCAULT, Michel. **Microfísica do poder**. 11. ed. São Paulo: Paz e Terra, 2021.

HAN, Byung-Chul. **Sociedade da transparência**. Petrópolis: Vozes, 2017.

MELO, Pedro Raphael Vieira. **Reconhecimento facial automatizado para fins de segurança pública e seus riscos aos titulares dos dados biométricos**. TCC (Graduação em Direito) – Instituto Brasileiro de Ensino, Desenvolvimento e Pesquisa, Brasília, 2020. Disponível em: https://repositorio.idp.edu.br/handle/123456789/3523. Acesso em: 24 jul. 2025.

MUNHOZ, Carina. **O *big data* e a ciência de dados na produção bibliográfica brasileira da biblioteconomia e da ciência da informação**. 2022. Dissertação (Mestrado em Ciência da Informação) – Universidade Federal Fluminense, Niterói, 2022. Disponível em: https://app.uff.br/riuff/handle/1/26746. Acesso em: 23 jul. 2025.

SANTOS, Lucas Gabriel de Matos; COSTA, Arthur Barbosa da; DAVID, Jéssica da Silva; PEDRO, Rosa Maria Leite Ribeiro. Reconhecimento facial: tecnologia, racismo e construção de mundos possíveis. **Psicologia & Sociedade**, Belo Horizonte, v. 35, *[s.n.]*, e277141, 2023. Disponível em: https://www.scielo.br/j/psoc/a/wJFV8yjBBr7cYnm3q6SXDjF/abstract/?lang=pt. Acesso em: 25 jul. 2025.

SÃO PAULO. **SMART SAMPA**: relatório de transparência. São Paulo: Prefeitura de São Paulo, 2025. Disponível em: https://smartsampa.prefeitura.sp.gov.br/relatorio_transparencia_smart_sampa.pdf. Acesso em: 21 jul. 2025.

SUPERIOR TRIBUNAL DE JUSTIÇA. **Recurso Especial nº 1.224.151 - CE**. Relator: Min. Cesar Asfor Rocha. Brasília, 09 ago. 2011. Disponível em: https://scon.stj.jus.br/SCON/GetInteiroTeorDoAcordao?num_registro=201002209912&dt_publicacao=06/09/2011. Acesso em: 29 jul. 2025.

YOSHIDA, Ernesto. As máquinas podem ser racistas? Como evitar a discriminação algorítmica. **Insper**, São Paulo, 22 fev. 2022. Disponível em: https://www.insper.edu.br/pt/noticias/2022/2/as-maquinas-podem-ser-racistas--como-evitar-a-discriminacao-algo. Acesso em: 25 jul. 2025.