IX ENCONTRO VIRTUAL DO CONPEDI

DIREITO, GOVERNANÇA E NOVAS TECNOLOGIAS V

D598

Direito, governança e novas tecnologias V [Recurso eletrônico on-line] organização CONPEDI

Coordenadores: Vivianne Rigoldi; Jéssica Fachin; Rosane Teresinha Porto – Florianópolis: CONPEDI, 2026.

Inclui bibliografia
ISBN: 978-65-5274-589-7
Modo de acesso: www.conpedi.org.br em publicações
Tema: Constituição, Processo e Justiça Social: o papel da jurisdição constitucional na efetivação de direitos

2. Direito. 3. Governança e novas tecnologias. IX Encontro Virtual do CONPEDI (2: 2026: Florianópolis, Brasil).

CDU: 34

Conselho Nacional de Pesquisa
e Pós-Graduação em Direito Florianópolis
Santa Catarina – Brasil
www.conpedi.org.br

IX ENCONTRO VIRTUAL DO CONPEDI

DIREITO, GOVERNANÇA E NOVAS TECNOLOGIAS V

Apresentação

O Conselho Nacional de Pesquisa e Pós-graduação em Direito (CONPEDI), referência na difusão de pesquisas que abordam os novos fenômenos envolvendo o Direito, firma-se como espaço qualificado para apresentação de pesquisas produzidas na área das novas tecnologias em face do Direito.

O tema, recorrente nos artigos apresentados - o uso da inteligência artificial no âmbito jurídico, demonstra que a maior sociedade científica na área jurídica do Brasil se mantém atenta às inovações tecnológicas, ao avanço de diversas tecnologias, novas experiências no judiciário e nos escritórios de advocacia. Artigos, de alta relevância acadêmica e científica, destacam que o Direito não está imune a essas transformações e reiteram a necessidade de atenção aos desafios regulatórios do uso da inteligência artificial no mundo jurídico.

Diferentes pesquisas, apresentadas no Grupo de Trabalho 'Direito, Governança e Novas Tecnologias V', alertam para os efeitos deletérios da opacidade algorítmica,

referindo-se à falta de transparência sobre como sistemas de inteligência artificial e seus algoritmos produzem decisões, dentro e fora do judiciário. Nos textos, a governança

digital é debatida, com rigorosa visão científica, objetivando garantir o uso estratégico de tecnologias de informação e comunicação para gerir serviços, promover a segurança

de dados e integrar processos, de forma transparente, eficiente, com foco na participação ativa do cidadão na tomada de decisões.

algorítmico e tecnológico do sistema de justiça, englobando a investigação de cibercrimes, a digitalização de procedimentos policiais e judiciais, provas digitais e a

regulação de plataformas para combater conteúdos ilícitos.

Destarte, os artigos apresentados e os debates produzidos no Grupo de Trabalho ‘Direito, Governança e Novas Tecnologias V’ são essenciais para o

fortalecimento das diretrizes nacionais de regulação das novas tecnologias, pela formação de parâmetros normativos e procedimentais adequados à proteção dos

direitos humanos e fundamentais, à garantia da segurança da informação, à gestão de riscos e ao fortalecimento da transparência e do alinhamento legal no uso das novas

tecnologias no âmbito jurídico.

Por essas razões, as coordenadoras do GT convidam para a leitura do teor integral dos artigos, agradecendo a participação dos autores pesquisadores desta edição.

Vivianne Rigoldi/Jéssica Fachin/Rosane Porto

O PANÓPTICO DIGITAL: IMPACTO DA INTELIGÊNCIA ARTIFICIAL NA LIBERDADE E PRIVACIDADE

THE DIGITAL PANOPTICON: THE IMPACT OF ARTIFICIAL INTELLIGENCE ON FREEDOM AND PRIVACY

Marianna Campos Diniz Do Amaral Ribeiro Santiago [1]
Carlos Alberto Rohrmann [2]

Resumo

Este artigo analisa criticamente o impacto da Inteligência Artificial sobre os direitos fundamentais à liberdade e à privacidade. O conceito de panóptico digital é utilizado como chave interpretativa para compreender a arquitetura de controle social viabilizada por sistemas algorítmicos. A pesquisa parte da hipótese de que a insuficiência dos marcos regulatórios vigentes converte a IA em vetor de consolidação de uma estrutura de vigilância onipresente, incompatível com os pressupostos do Estado Democrático de Direito. O trabalho examina como a opacidade decisória, o viés algorítmico e a coleta massiva de dados biométricos se manifestam em setores críticos da sociedade, consolidando um paradigma de monitoramento contínuo do espaço comum. Três casos de relevância jurídica comprovada são analisados: o falso positivo no caso de Robert Williams nos Estados Unidos, a vigilância biométrica em massa no programa Smart Sampa de São Paulo e a extração predatória de imagens no caso Clearview AI. Os casos demonstram que os riscos identificados não são hipotéticos, mas produzem violações concretas e juridicamente mensuráveis de direitos fundamentais. A análise dos marcos regulatórios europeus, com ênfase no GDPR e no AI Act, e do ordenamento jurídico brasileiro, a partir da LGPD e do PL 2.338/2023, revela insuficiências estruturais que apontam para a necessidade de um marco normativo específico, preventivo e constitucionalmente adequado para o uso de reconhecimento facial pelo Estado. A pesquisa emprega método dedutivo, de natureza qualitativa e aplicada, combinando revisão bibliográfica e documental com o estudo de casos múltiplos e emblemáticos.

Palavras-chave: Inteligência artificial, Privacidade, Liberdade, Direitos fundamentais,

The research starts from the hypothesis that the insufficiency of existing regulatory frameworks converts AI into a vector for consolidating a pervasive surveillance structure incompatible with the principles of the Democratic Rule of Law. The study examines how decision-making opacity, algorithmic bias, and the mass collection of biometric data manifest in the public security sector, consolidating a paradigm of continuous monitoring of shared spaces. Three cases of proven legal relevance are analyzed: the false positive in the Robert Williams case in the United States, the mass biometric surveillance of São Paulo's Smart Sampa program, and the predatory extraction of images in the Clearview AI case. The cases demonstrate that the identified risks are not hypothetical, but produce concrete and legally measurable violations of fundamental rights. The analysis of European regulatory frameworks, with emphasis on the GDPR and the AI Act, and of the Brazilian legal system, based on the LGPD and Bill 2,338/2023, reveals structural shortcomings pointing to the need for a specific, preventive, and constitutionally adequate regulatory framework for the use of facial recognition by the State. The research employs a deductive method, qualitative and applied in nature, combining bibliographic and documentary review with the study of multiple emblematic cases.

Keywords/Palabras-claves/Mots-clés: Artificial intelligence, Privacy, Freedom, Fundamental rights, Digital panopticon

INTRODUÇÃO

A Inteligência Artificial (IA) transcendeu definitivamente o campo da ficção científica para se consolidar como uma infraestrutura tecnológica onipresente, remodelando as operações em praticamente todos os setores da sociedade contemporânea. Este trabalho busca investigar criticamente como a disseminação de sistemas algorítmicos, embora prometa eficiência e inovação, introduz simultaneamente riscos sistêmicos que ameaçam a autonomia individual e a própria estrutura do Estado Democrático de Direito, visando, em última análise, compatibilizar o avanço tecnológico com a salvaguarda dos direitos fundamentais.

Com efeito, a capacidade da IA de processar volumes massivos de dados, identificar padrões e automatizar decisões em escala sobre-humana gera o substrato para dilemas éticos e jurídicos de enorme complexidade. Fenômenos como a opacidade decisória, o viés algorítmico e a coleta de dados biométricos em larga escala não são falhas isoladas, mas características que, ao convergirem, consolidam um novo e sem precedentes paradigma de vigilância. Abordar essas questões é, portanto, essencial não apenas para assegurar que a tecnologia contribua para uma sociedade mais justa, mas para promover a confiança pública em suas aplicações e garantir a proteção da dignidade humana.

A pesquisa tem como objetivo geral analisar criticamente o impacto multifacetado da Inteligência Artificial sobre os direitos à liberdade e à privacidade na sociedade contemporânea. Especificamente, busca-se: examinar as aplicações da IA no setor de segurança pública, identificando os riscos estruturais que o uso de reconhecimento facial impõe à liberdade e à privacidade; aprofundar o conceito de "Panóptico Digital" como ferramenta teórica para compreender a nova dinâmica de vigilância; examinar, por meio de estudos de caso, as consequências concretas da implementação não regulada dessa tecnologia; avaliar criticamente a adequação dos marcos regulatórios vigentes frente aos riscos documentados; e fundamentar a urgência do debate sobre a governança ética e jurídica da Inteligência Artificial.

A hipótese central deste trabalho pressupõe que a insuficiência dos marcos regulatórios vigentes e de mecanismos de *accountability* efetivos converte a Inteligência Artificial em uma ferramenta de poder que, em vez de atuar como um instrumento neutro, funciona como um catalisador para a consolidação de um "Panóptico Digital". Argumenta-se que essa estrutura de vigilância onipresente e invisível normaliza o monitoramento e o controle comportamental dos cidadãos no espaço público, ameaçando diretamente os pilares da liberdade, da privacidade e da dignidade humana em uma sociedade democrática.

Este estudo se baseia primordialmente no conceito de "Panóptico", concebido por Jeremy Bentham no século XVIII e reinterpretado por Michel Foucault (2014) como modelo do poder disciplinar que opera pela internalização da vigilância. O conceito é aqui atualizado para a era digital a fim de descrever a arquitetura de controle social viabilizada pela IA. Essa análise é complementada pelas teorias de Shoshana Zuboff (2021) sobre o "capitalismo de vigilância" e de Frank Pasquale (2015) sobre a "sociedade da caixa preta". A expectativa é que o estudo revele os desafios de regular a IA, demonstrando que a governança da tecnologia não é apenas uma questão técnica, mas uma tensão política e filosófica cuja resolução impacta diretamente a autonomia individual e a democracia.

Para tanto, a presente pesquisa emprega o método de abordagem dedutivo, com natureza qualitativa e aplicada. Os procedimentos técnicos para a consecução dos objetivos propostos combinam a pesquisa bibliográfica e documental, com a análise aprofundada de artigos acadêmicos, legislação pertinente, relatórios de organizações internacionais e publicações especializadas sobre o tema, bem como a análise crítica dos principais marcos regulatórios em vigor. Adicionalmente, a investigação se vale do estudo de casos múltiplos e emblemáticos (o erro de identificação no caso de Robert Williams, a vigilância biométrica no programa Smart Sampa da cidade de São Paulo e a extração predatória de imagens no caso Clearview AI), como ferramenta para ilustrar empiricamente e fundamentar a análise crítica sobre o impacto da Inteligência Artificial nos direitos fundamentais.

1 A INTELIGÊNCIA ARTIFICIAL NA SEGURANÇA PÚBLICA: EFICIÊNCIA OPERACIONAL E RISCOS ESTRUTURAIS

A utilização da Inteligência Artificial pelo setor público e pelas agências de segurança representa, dentre os setores em que a IA opera, aquela com maior potencial de impacto sobre os direitos fundamentais à liberdade e à privacidade. Isso porque, nesse contexto, o Estado, detentor do monopólio legítimo da força, passa a dispor de uma infraestrutura tecnológica que converte o espaço público em um ambiente de monitoramento contínuo e praticamente inescapável. Sob o argumento da eficiência operacional e da responsabilidade constitucional pela garantia da segurança pública, governos têm investido crescentemente em sistemas de reconhecimento facial, vigilância urbana em rede e policiamento preditivo, tecnologias que, individualmente e em conjunto, reconfiguram profundamente a relação entre o Estado e os cidadãos.

O reconhecimento facial é a tecnologia mais emblemática dessa transformação. Ao contrário de outros instrumentos de vigilância, ele opera de forma remota, passiva e imperceptível: um indivíduo que simplesmente transita por um espaço público pode ter sua

identidade capturada, registrada e cruzada com bancos de dados governamentais sem que tome qualquer ciência disso e sem que tenha oferecido qualquer consentimento. Como destaca Qandeel (2024), em análise publicada pela *Frontiers in Big Data*, a coleta de dados biométricos por meio do reconhecimento facial é estruturalmente distinta de outras formas de coleta de dados pessoais: o rosto humano é um dado permanente, imutável e publicamente exposto, cuja captura e armazenamento elimina qualquer expectativa razoável de privacidade no espaço comum. Uma senha comprometida pode ser alterada; o registro de uma face indevidamente capturado, jamais.

Essa arquitetura de vigilância produz aquilo que a doutrina denomina *chilling effect*: a mera possibilidade de ser identificado e monitorado no espaço público é suficiente para induzir a autocensura e condicionar o comportamento dos cidadãos. Quando o agente vigilante é o Estado, esse efeito não recai apenas sobre escolhas cotidianas, mas sobre o exercício de liberdades políticas fundamentais, como o direito de reunião, de manifestação e de associação. É precisamente aqui que o Panóptico Digital encontra sua manifestação mais concreta: não é necessário que a vigilância seja constante para que produza seus efeitos disciplinares, basta que o cidadão saiba que ela é possível (Foucault, 2014).

Agrava esse quadro o fato de que os dados biométricos coletados por sistemas estatais frequentemente transitam por circuitos opacos, sendo compartilhados com empresas privadas, outros órgãos governamentais ou mesmo cedidos a terceiros sem o conhecimento dos cidadãos. Qandeel (2024) ressalta que os marcos regulatórios existentes mostram-se progressivamente insuficientes para abarcar as especificidades do reconhecimento facial em espaços públicos, sobretudo no que diz respeito à definição de consentimento válido, à limitação de finalidade e à responsabilização em casos de uso indevido.

Nessa direção, o European Data Protection Board (EDPB, 2023), em diretrizes específicas sobre o uso de reconhecimento facial por autoridades policiais, reconheceu que essa tecnologia representa uma interferência particularmente severa nos direitos fundamentais, recomendando que sua utilização seja condicionada a critérios estritos de necessidade e proporcionalidade.

2 O PANÓPTICO DIGITAL: RISCOS PARA A LIBERDADE E PRIVACIDADE

2.1 O Panóptico de Bentham e a Teoria do Poder Disciplinar de Foucault

A vigilância sempre esteve presente como mecanismo de controle social, porém sua abrangência foi historicamente limitada pelo custo de observar. Vigiar exigia presença física, agentes e recursos, de modo que o monitoramento era necessariamente seletivo e essa

seletividade funcionava, ainda que de forma involuntária, como barreira ao poder de quem vigia (Foucault, 2014).

Foi justamente para superar essa limitação que Jeremy Bentham concebeu, em 1785, o Panóptico, uma prisão circular dotada de uma torre central de observação, a partir da qual um único vigilante poderia monitorar todas as celas sem que os presos soubessem se estavam sendo de fato observados. A eficiência do modelo residia, portanto, na inversão da lógica tradicional de controle, pois bastava que o vigiado conhecesse a possibilidade de estar sendo observado para que a incerteza permanente o conduzisse à autodisciplina, tornando o poder mais eficaz na medida em que se tornava menos visível (Bentham, 1791).

Michel Foucault retomou esse projeto como metáfora do poder disciplinar moderno, argumentando que o efeito central do Panóptico não é a punição, mas sim a interiorização da vigilância pelo próprio vigiado. Enquanto o poder soberano se manifestava por meio de punições espetaculares, o poder disciplinar opera de forma contínua, capilar e invisível, moldando condutas pela normalização. Dessa forma, o controle deixa de ser exercido de fora para dentro e passa a operar de dentro para fora, o que constitui o fundamento da sociedade disciplinar descrita por Foucault (2014).

2.2 O Panóptico Digital: Vigilância Algorítmica Onipresente

Na contemporaneidade, sistemas de reconhecimento facial, algoritmos de análise comportamental, dispositivos conectados em rede e plataformas digitais tornaram possível coletar, armazenar e cruzar dados sobre milhões de pessoas simultaneamente, de forma contínua e a custo marginal praticamente nulo (Zuboff, 2021). A vigilância deixou de ser um ato físico, visível e direcionado para se tornar um processo algorítmico, invisível e onipresente. A Inteligência Artificial industrializou essa lógica, tornando o monitoramento escalável, contínuo e estrutural, não mais uma prática excepcional justificada caso a caso, mas a condição ordinária da vida social contemporânea (Duke, 2023).

O Panóptico de Bentham tinha limites físicos precisos: uma prisão, uma torre, muros. O Panóptico Digital não tem paredes. Assistentes de voz, smartphones, relógios inteligentes, dispositivos conectados em rede, cada um desses objetos é um sensor permanentemente ativo, capaz de captar, processar, armazenar e transmitir dados sobre seus usuários de forma contínua e imperceptível. Andrejevic (2019) sintetiza com precisão essa ruptura: a pontualidade do Panóptico original, que operava pela incerteza de ser observado, é substituída pela lógica oposta, a da monitorização abrangente e permanente, distribuída por redes de sensores incorporados ao cotidiano. O que antes exigia uma prisão, hoje habita a sala de estar.

Esse aparato invisível e distribuído é o que Zuboff (2015) denomina "*Big Other*", uma infraestrutura de vigilância descentralizada e automatizada que permeia toda interação digital, sem a face coercitiva do poder soberano, mas com efeitos equivalentes sobre o comportamento e a liberdade. Han (2018) acrescenta a dimensão mais perturbadora dessa dinâmica: ao contrário dos presos de Bentham, que resistiam ao olhar da torre, os habitantes do Panóptico Digital constroem voluntariamente as paredes de sua própria prisão, ao instalar dispositivos, aceitar termos de uso e compartilhar dados em troca de conveniência. O controle torna-se total precisamente porque dispensa a coerção: o vigiado é também cúmplice ativo da sua própria vigilância.

Os dados produzidos por essa arquitetura representam um recurso de poder sem precedentes. Estados e corporações convergem progressivamente no acesso e no uso dessas infraestruturas de monitoramento, apagando a fronteira entre vigilância comercial e vigilância política (Zuboff, 2021). Essa lógica de controle invisível e onipresente, até aqui examinada em seus fundamentos conceituais, deixa de ser abstração quando confrontada com suas manifestações empíricas. A próxima seção analisa três casos documentados que expõem como a arquitetura panóptica digital já opera, na prática, como vetor de violações de direitos fundamentais.

3 ESTUDOS DE CASO: AS MÚLTIPLAS FACES DA VIOLAÇÃO DE DIREITOS

Esta seção examina três casos documentados nos quais a vigilância algorítmica se materializou em violações concretas de direitos fundamentais. A tecnologia de reconhecimento facial constitui o fio condutor precisamente porque concentra, em uma única aplicação, todas as dimensões de risco até aqui examinadas: viés sistêmico, coleta massiva de dados biométricos sem consentimento e uso como instrumento de controle comercial e político. Os casos a seguir não foram selecionados por seu valor ilustrativo, mas por sua relevância jurídica comprovada e por terem gerado literatura acadêmica e decisões regulatórias de reconhecida credibilidade, tornando-os referências no debate sobre governança da inteligência artificial.

3.1 O Caso Robert Williams e a Falibilidade da Identificação Automatizada

O caso de Robert Williams, ocorrido em janeiro de 2020 no Michigan, Estados Unidos, constitui um marco sobre os riscos da automação na persecução penal. Williams, um homem negro, foi detido sob acusação de furto qualificado em uma loja de artigos de luxo em Detroit após um sistema de reconhecimento facial gerar uma correspondência positiva a partir de imagens de vigilância de baixa resolução. Após trinta horas de custódia, os próprios investigadores reconheceram que se tratava de erro de identificação.

A ação *Williams v. City of Detroit et al.*, ajuizada pela ACLU of Michigan na condição de representante judicial de Williams perante o Tribunal Federal do Distrito Leste do Michigan (Caso n.º 2:21-cv-10827-LJM-DRG), culminou em junho de 2024 em acordo homologado pela Juíza Federal Laurie J. Michelson, pelo qual a Cidade de Detroit comprometeu-se a reformar radicalmente sua política de uso da tecnologia, vedando o uso do reconhecimento facial como fundamento exclusivo para prisões ou pedidos de mandado de prisão (Estados Unidos, 2024).

A falha no caso Williams não representou um desvio isolado, mas uma vulnerabilidade estrutural. O National Institute of Standards and Technology (NIST), agência federal do Departamento de Comércio dos Estados Unidos, publicou em dezembro de 2019 o relatório técnico *Face Recognition Vendor Test (FRVT) — Part 3: Demographic Effects* (NIST IR 8280). O documento resulta da avaliação direta de 189 algoritmos de reconhecimento facial submetidos por desenvolvedores de todo o mundo e constatou que a maioria dos sistemas de origem norte-americana produzia taxas de falsos positivos entre 10 e 100 vezes maiores para rostos de pessoas negras e asiáticas em comparação a indivíduos brancos (NIST, 2019).

A causa fundamental dessa disparidade reside na composição dos conjuntos de dados de treinamento. Um dos repositórios mais utilizados globalmente pela indústria e pela academia é o *Labeled Faces in the Wild* (LFW), biblioteca digital que reúne fotografias capturadas de fontes públicas na internet e que apresenta sobrerrepresentação de 83,5% de imagens de pessoas brancas (NIST, 2019).

Como o sistema é treinado majoritariamente com perfis de pele clara, ele desenvolve alta performance na extração de características desses indivíduos, tornando-se capaz de distinguir detalhes mínimos entre rostos brancos. Em relação a grupos sub-representados, contudo, o algoritmo não recebe exemplos suficientes para aprender a diferenciar nuances individuais, tendendo a agrupar rostos distintos em um mesmo padrão genérico. Em termos técnicos, essa desproporção gera um viés de representatividade.

Consequentemente, o software apresenta uma tendência matemática de gerar falsos positivos: quando o sistema identifica erroneamente duas pessoas diferentes como sendo a mesma. No caso de Robert Williams, o algoritmo, treinado de forma deficitária, não foi capaz de diferenciar o seu rosto daquele capturado pela câmera de segurança, transformando uma deficiência de engenharia de dados em fundamento direto para uma indevida restrição de liberdade.

O desfecho do caso Williams é paradigmático para a governança regulatória. Em junho de 2024, a Cidade de Detroit celebrou um acordo histórico de USD 300.000, sendo compelida a reformar radicalmente sua política de uso da tecnologia: a Polícia de Detroit ficou expressamente proibida de conduzir reconhecimento fotográfico baseado exclusivamente em resultado de sistema automatizado, bem como de solicitar mandado de prisão sem evidência independente que corrobore a identificação (Estados Unidos, 2024). O caso influenciou a legislação no estado da Califórnia e é hoje referência central no debate sobre os limites constitucionais do uso de inteligência artificial no sistema de justiça criminal.

Diante desse substrato técnico, Cebreros (2025) demonstra que o caso Williams não é uma exceção, mas o primeiro caso documentado de uma série: pelo menos sete prisões injustas por erros de reconhecimento facial foram registradas nos Estados Unidos nos anos subsequentes, afetando desproporcionalmente homens e mulheres negros. A análise jurídica da autora, publicada no *Washington Law Review Online*, demonstra que em todos esses casos a polícia descumpriu seus próprios protocolos internos, que proibiam o uso do reconhecimento facial como único fundamento para uma prisão. A tecnologia, portanto, não atuou como uma ferramenta de investigação sujeita ao escrutínio humano, mas como uma autoridade que substituiu a investigação policial tradicional.

3.2 O Smart Sampa e os Limites da Vigilância Biométrica no Ordenamento Jurídico Brasileiro

Se o caso Williams ilustra as consequências do erro algorítmico sobre o indivíduo, o programa Smart Sampa, implementado pela Prefeitura de São Paulo a partir de 2023, permite examinar como a mesma tecnologia opera em escala urbana dentro de um Estado Democrático de Direito. O programa, atualmente, integra mais de 40 mil câmeras conectadas a um centro de controle operacional com capacidade de reconhecimento facial em tempo real, constituindo o maior sistema de vigilância biométrica da América Latina (São Paulo, 2025a).

A implementação do Smart Sampa coloca em tensão dois valores constitucionais. De um lado, a segurança pública, prevista no art. 144, *caput*, da Constituição Federal (Brasil, 1988). De outro, o direito à proteção de dados pessoais, elevado à condição de direito fundamental pelo art. 5º, LXXIX, inserido pela Emenda Constitucional n.º 115/2022.

Em ação popular ajuizada perante a 3ª Vara da Fazenda Pública de São Paulo, o Juiz Luis Manuel Fonseca Pires deferiu liminar suspendendo o processo licitatório do Smart Sampa ao reconhecer, nos autos do processo n.º 1027876-45.2023.8.26.0053, que a ausência de regulação legal prévia impedia a contratação e que o sistema apresentava risco de reprodução de desigualdades estruturais de forma automatizada (São Paulo, 2023a).

A decisão foi, posteriormente, reformada pelo acórdão da 3ª Câmara de Direito Público do TJSP, proferido no Agravo de Instrumento n.º 2122169-52.2023.8.26.0000, sob o fundamento de que a LGPD não se aplica ao tratamento de dados para fins de segurança pública, nos termos do art. 4º, III, "a" e "d", da Lei n.º 13.709/2018 (São Paulo, 2023b).

Essa lacuna normativa é, como observa Zucchetti Filho (2025), o principal vetor de insegurança jurídica do programa: ele opera em uma zona em que os princípios da finalidade, da necessidade e da não discriminação previstos no art. 6º da LGPD não incidem diretamente sobre a atuação policial.

Os dados produzidos pelo próprio poder público indicam que os riscos não são abstratos. O Relatório de Transparência do Smart Sampa, publicado pela Secretaria Municipal de Segurança Urbana e referente ao período de novembro de 2024 a maio de 2025, registrou 82 abordagens policiais decorrentes de alertas do sistema. Desse total, 23 corresponderam a falsos positivos, representando 28,05% das abordagens computadas (São Paulo, 2025b).

Esse índice reflete a mesma vulnerabilidade estrutural documentada pelo NIST no contexto norte-americano, agravada pelo fato de que o programa não divulga publicamente o tipo de software utilizado, a margem de erro desagregada por grupo demográfico nem os critérios de compartilhamento dos dados com outros órgãos (Zucchetti Filho, 2025).

O *chilling effect* produzido por essa arquitetura de vigilância vai além das abordagens formalmente registradas, uma vez que o reconhecimento facial opera de forma contínua no espaço público, a mera possibilidade de identificação equivocada é suficiente para condicionar o comportamento dos cidadãos, tal como descreve Foucault (2014) ao analisar o efeito disciplinar do Panóptico. Assim, quando esse agente vigilante é o Estado, a autocensura incide não apenas sobre escolhas cotidianas, mas sobre o exercício de liberdades políticas fundamentais, como o direito de reunião e de manifestação, previstos no art. 5º, XVI e XVII, da Constituição Federal (Brasil, 1988).

3.3 A Extração Predatória de Dados e o Fim do Anonimato Digital: O Caso Clearview AI

Enquanto os casos anteriores examinam a vigilância biométrica exercida diretamente pelo Estado, o caso da empresa norte-americana Clearview AI expõe a dimensão que a torna possível: a construção privada de uma infraestrutura de identificação biométrica global que, ao ser comercializada a agências de segurança pública, converte garantias constitucionais em letra morta. Se o ato originário de vigilância é praticado por um agente privado, os limites que o direito constitucional impõe ao Estado tornam-se inoperantes. É precisamente essa

convergência entre vigilância privada e estatal que faz do caso Clearview AI um estudo indispensável no recorte desta pesquisa.

Fundada em 2017 e sediada em Nova York, a Clearview AI desenvolveu um sistema automatizado de raspagem de dados (*web scraping*) que coletou, de forma indiscriminada, bilhões de imagens faciais a partir de redes sociais e websites publicamente acessíveis, sem o conhecimento ou consentimento dos indivíduos retratados. A partir dessas imagens, a empresa construiu um banco de dados biométrico que, em 2022, já reunia mais de 20 bilhões de fotografias, e comercializava o acesso a esse repositório como ferramenta de identificação facial para agências de segurança pública e entidades privadas (CNIL, 2022). A premissa jurídica invocada pela empresa era a de que imagens publicadas na internet seriam dados de domínio público, cujo uso dispensaria consentimento.

Em resposta, autoridades de proteção de dados da Europa, do Canadá e dos Estados Unidos impuseram severas sanções à empresa, consolidando um entendimento comum contra a vigilância em massa. Decisões de agências europeias e canadenses (Garante, 2022; CNIL, 2022; 2023; ICO, 2022; 2025; OPC, 2021; 2021a) convergiram na tese de que a coleta massiva e indiscriminada de dados biométricos faciais configura tratamento ilícito. Essas autoridades rejeitaram expressamente o argumento de que a disponibilidade pública das imagens na internet dispensaria o consentimento dos titulares ou a exigência de uma base legal. Esse cerco regulatório foi reforçado nos Estados Unidos, onde litígios judiciais (Estados Unidos, 2022; Estados Unidos, 2025) resultaram não apenas em pesados acordos financeiros, mas também em decisões que proibiram permanentemente a empresa de conceder acesso ao seu banco de dados para entidades privadas.

A convergência dessas decisões em jurisdições tão distintas consolida um princípio normativo de alcance global: a publicidade de um dado na internet não equivale à renúncia ao controle sobre as finalidades de seu tratamento. Como sustenta Qandeel (2024), o caso Clearview AI representa uma ruptura qualitativa no campo das violações de privacidade, pois a infraestrutura de vigilância foi deliberadamente construída sobre a premissa da apropriação predatória de dados publicamente acessíveis. A autora argumenta que esse cenário impõe a transição de um modelo de mera autorregulação corporativa para um regime de responsabilidade jurídica estrita, reforçando que o Estado de Direito não pode tolerar que a disponibilidade pública de dados pessoais sirva de fundamento para o seu processamento biométrico indiscriminado e comercialmente orientado.

4 A INSUFICIÊNCIA DOS MARCOS REGULATÓRIOS VIGENTES

4.1 O GDPR e o Consentimento Informado

Estabelecidas as bases técnicas da vigilância algorítmica e as violações concretas advindas de sua aplicação, impõe-se a análise do aparato jurídico destinado a contê-la. O Regulamento (UE) 2016/679, conhecido como *General Data Protection Regulation* (GDPR), entrou em vigor em 25 de maio de 2018 e consolidou-se como referência global em matéria de proteção de dados pessoais. Seu artigo 5º estabelece princípios como licitude, transparência, limitação de finalidade, minimização da coleta e responsabilização (*accountability*), pelos quais os responsáveis pelo tratamento devem demonstrar conformidade de forma ativa e verificável (União Europeia, 2016). Contudo, o exame de sua aplicação revela um descompasso estrutural, pois as salvaguardas tradicionais do direito à privacidade, notadamente o consentimento e a transparência, enfrentam uma crise de eficácia diante da complexidade dos sistemas contemporâneos.

O consentimento do titular foi elevado à condição de manifestação de vontade livre, informada, específica e inequívoca (União Europeia, 2016, art. 4º, n. 11). Contudo, na prática, essa exigência é estruturalmente comprometida. Acquisti, Brandimarte e Loewenstein (2015) demonstraram que os usuários raramente leem políticas de privacidade, não compreendem as implicações do compartilhamento de dados e subestimam os riscos da cessão de informações pessoais. Na sociedade em rede, a alternativa ao consentimento é a exclusão digital, o que configura não uma escolha genuína, mas uma forma velada de coerção.

Agrava esse cenário o fenômeno do *purpose creep*, isto é, a reutilização de dados para finalidades diversas daquelas declaradas no momento da coleta, em violação ao princípio da limitação de finalidade consagrado no Artigo 5º, alínea b, do GDPR (União Europeia, 2016). Como já alertava Solove (2008), as arquiteturas informacionais modernas criam estruturas de poder que escapam à compreensão dos próprios titulares. A transparência, por sua vez, revela-se igualmente ilusória, pois a grande maioria dos titulares desconhece os mecanismos pelos quais seus dados são coletados, transferidos e processados algoritmicamente.

Essa opacidade, contudo, não é meramente estratégica. Mittelstadt *et al.* (2016) identificam dimensões técnica, intencional e de escala na opacidade algorítmica, argumentando que, em modelos de aprendizado de máquina de alta complexidade, a explicabilidade torna-se um problema mesmo para os próprios desenvolvedores. Nesse contexto, o debate jurídico buscou balizas normativas e consolidou a expressão "direito à explicação" (*right to explanation*), a partir da tese de Goodman e Flaxman (2017), segundo a qual o GDPR imporia o dever de esclarecer a lógica individualizada de decisões automatizadas.

Essa interpretação, porém, é alvo de severa contestação. Wachter, Mittelstadt e Russell (2017) demonstram que o termo carece de literalidade no corpo vinculante do regulamento, uma vez que o Artigo 22 assegura apenas o direito à intervenção humana e à contestação, enquanto a menção à "explicação" restringe-se ao Considerando 71, de caráter meramente interpretativo. Dessa forma, a norma europeia estabelece, no máximo, um "direito a ser informado" sobre a lógica geral do sistema, revelando um hiato entre a expectativa de transparência e a proteção efetivamente positivada.

Na prática, os direitos formalmente reconhecidos pelo GDPR são frequentemente contornados por mecanismos técnicos sofisticados. Estudos empíricos demonstraram que interfaces de consentimento continuam amplamente recorrendo a *dark patterns*, padrões de design que manipulam as escolhas dos usuários, para induzir consentimentos que não refletem preferências genuínas (Nouwens *et al.*, 2020; Mathur *et al.*, 2019). Paralelamente, a invocação do segredo comercial como barreira ao escrutínio externo sobre algoritmos constitui prática documentada que Pasquale (2015) identifica como estrutural ao modelo das grandes plataformas digitais.

Consolida-se, assim, a assimetria de poder que atravessa toda a análise: corporações e governos acumulam conhecimento granular sobre indivíduos, enquanto estes permanecem alheios às decisões que sobre eles incidem (Nissenbaum, 2010). O titular dos dados é progressivamente reduzido a mero objeto de predição.

4.2 O *AI Act*: Avanços e Limitações Estruturais

As violações examinadas neste artigo evidenciam que o GDPR não foi concebido para enfrentar a totalidade dos riscos impostos pela Inteligência Artificial. O reconhecimento dessa lacuna levou a União Europeia a aprovar, em junho de 2024, o Regulamento (UE) 2024/1689, denominado *AI Act*, que entrou em vigor em 1º de agosto de 2024 e cujas primeiras regras proibitivas tornaram-se aplicáveis em 2 de fevereiro de 2025.

O *AI Act* constitui o primeiro marco regulatório abrangente e juridicamente vinculante especificamente voltado à Inteligência Artificial no mundo. Sua arquitetura normativa estrutura-se sobre uma abordagem baseada em risco, que classifica os sistemas de IA em quatro categorias: risco inaceitável, cujas práticas são expressamente proibidas; alto risco, sujeito a obrigações regulatórias rigorosas; risco limitado, ao qual se impõem deveres de transparência; e risco mínimo ou nulo, isento de regulação específica. Essa gradação permite calibrar a intervenção estatal à gravidade potencial de cada aplicação, evitando tanto a sub-regulação de sistemas perigosos quanto a restrição desnecessária à inovação (União Europeia, 2024).

Os avanços introduzidos pelo regulamento são significativos e respondem diretamente a vários dos problemas documentados neste artigo. O artigo 5º, alínea (e), proíbe de forma absoluta, sem admitir exceções, a criação ou expansão de bancos de dados de reconhecimento facial por meio de coleta indiscriminada (*untargeted scraping*) de imagens da internet ou de filmagens de circuito fechado. Essa disposição confronta diretamente o modelo de negócios que viabilizou a operação da Clearview AI, cuja base de dados, conforme demonstrado na seção 3, foi construída precisamente por meio dessa prática.

Na mesma direção, o artigo 5º, alínea (g), veda a utilização de sistemas de categorização biométrica que infiram raça, opinião política, filiação sindical, convicções religiosas ou orientação sexual. O artigo 5º, alínea (h), complementa esse quadro ao estabelecer a proibição, em princípio, do uso de sistemas de identificação biométrica remota em tempo real em espaços publicamente acessíveis para fins de aplicação da lei. As exceções admitidas são limitadas e condicionadas a autorização judicial prévia, avaliação de impacto sobre direitos fundamentais e registro em base de dados europeia.

Para além das proibições absolutas, o *AI Act* impõe obrigações específicas aos sistemas classificados como de alto risco que repercutem diretamente sobre os direitos à privacidade e à liberdade. O artigo 10 estabelece requisitos de governança e qualidade dos dados de treinamento, buscando mitigar vieses discriminatórios como o que comprometeu o sistema de reconhecimento facial utilizado no caso Williams. O artigo 13 impõe deveres de transparência que vão além do GDPR, incluindo informações sobre as limitações esperadas do sistema. Já o artigo 86 consagra expressamente o direito à explicação de decisões individuais tomadas com base em sistemas de alto risco que afetem direitos fundamentais.

Não obstante esses avanços, o *AI Act* apresenta limitações estruturais que comprometem sua capacidade de prevenir violações análogas às documentadas neste trabalho. A primeira delas reside na dependência significativa de autodeclaração e autoavaliação de conformidade pelos próprios fornecedores de sistemas, prevista no artigo 43, que relega a auditoria independente a uma minoria de casos. Esse modelo replica uma fragilidade já identificada no GDPR: empresas declaram conformidade formalmente, mas violações concretas só são identificadas anos depois, quando os danos já se consumaram, como se verificou tanto no caso Williams quanto na operação da Clearview AI.

A segunda limitação concerne às obrigações de transparência e explicabilidade que, embora mais detalhadas do que no GDPR, permanecem tecnicamente vagas, sem especificar métricas objetivas ou padrões auditáveis verificáveis. Ademais, há uma terceira limitação, de ordem territorial e política, que se manifesta nas amplas isenções para segurança nacional e

defesa. Essas exceções podem ser invocadas por Estados-membros para justificar exatamente o tipo de vigilância em massa documentada no caso do Smart Sampa, criando um precedente normativo que fragiliza a coerência do sistema de proteção.

Em síntese, o *AI Act* representa um avanço inegável ao inaugurar a regulação específica da Inteligência Artificial com instrumentos que, se tivessem existido anteriormente, poderiam ter prevenido ou mitigado algumas das violações analisadas ao longo deste artigo. Entretanto, suas limitações estruturais como a dependência de autoavaliação, a imprecisão das exigências de transparência e as amplas isenções de segurança, revelam que mesmo o marco regulatório mais avançado do mundo permanece aquém dos desafios que se propõe a enfrentar. Essa constatação reforça a tese central deste trabalho: a defasagem entre o ritmo de desenvolvimento tecnológico e a capacidade de resposta normativa persiste como um problema estrutural.

4.3 O Ordenamento Jurídico Brasileiro diante da Vigilância Biométrica: Lacunas, Omissões e Perspectivas Regulatórias

O exame dos marcos regulatórios europeus revela um contraste que não pode ser ignorado: enquanto o GDPR e o *AI Act* consolidam um arcabouço progressivamente mais rigoroso para o tratamento de dados biométricos, o Brasil enfrenta uma lacuna estrutural que o caso Smart Sampa expôs de forma concreta. Compreender essa lacuna exige partir da arquitetura normativa vigente e identificar com precisão onde ela falha.

A Lei n.º 13.709/2018, Lei Geral de Proteção de Dados Pessoais, representa o principal avanço do ordenamento jurídico brasileiro na matéria. A lei estabelece, em seu art. 6º, princípios que deveriam reger qualquer tratamento de dados pessoais: finalidade, adequação, necessidade, transparência e não discriminação. No entanto, o art. 4º, III, "a" e "d", exclui expressamente do âmbito de incidência da lei o tratamento de dados realizado para fins de segurança pública e persecução penal (Brasil, 2018). Essa exclusão, aplicada pelo Tribunal de Justiça de São Paulo no julgamento do Agravo de Instrumento n.º 2122169-52.2023.8.26.0000, significa que o sistema Smart Sampa opera em uma zona em que os princípios mais elementares de proteção de dados não incidem sobre a atuação policial (São Paulo, 2023b).

A própria LGPD reconhece a precariedade dessa solução: o parágrafo único do mesmo art. 4º determina que o tratamento de dados para fins de segurança pública deve ser regulado por legislação específica (Brasil, 2018). Essa lei específica, contudo, ainda não existe. Como observa Mendes *et al.* (2026), a ausência de regulamentação setorial para o uso de dados pessoais por autoridades policiais constitui um dos pontos mais críticos de

incompletude do sistema brasileiro de proteção de dados, criando um vácuo normativo que autoriza, na prática, o que a constituição exige que seja regulado. A autora demonstra que essa omissão não é neutra: ela distribui de forma desigual os riscos tecnológicos, recaindo desproporcionalmente sobre grupos historicamente vulneráveis à atuação do sistema de segurança.

Esse cenário ganhou nova dimensão com a Emenda Constitucional n.º 115/2022, que inseriu o art. 5º, LXXIX, na Constituição Federal, elevando a proteção de dados pessoais à condição de direito fundamental e impondo ao Estado o dever de garantir esse direito. A elevação constitucional do direito, contudo, não foi acompanhada da produção legislativa que ela exige. Três anos após a promulgação da emenda, o uso de reconhecimento facial por autoridades públicas segue sem disciplina legal específica, o que configura, em tese, uma omissão inconstitucional por parte do legislador (Brasil, 1988).

No plano infraconstitucional, a resposta mais relevante em curso é o Projeto de Lei n.º 2.338/2023, de autoria do Senador Rodrigo Pacheco, aprovado pelo Plenário do Senado Federal em dezembro de 2024 e atualmente em tramitação na Câmara dos Deputados (Brasil, 2023). O projeto adota abordagem baseada em risco, classifica os sistemas de IA conforme seu potencial de impacto sobre direitos fundamentais e prevê, em seu art. 13, que tecnologias de reconhecimento facial em espaços públicos são de risco excessivo. A tramitação, contudo, enfrenta resistências que evidenciam a tensão entre segurança e liberdade que percorre todo este artigo: o texto aprovado no Senado estabelece amplo rol de exceções para usos em segurança pública, que, na prática, abarcam a maioria das aplicações em operação no país, incluindo sistemas como o Smart Sampa (Brasil, 2023; Brasil, 2024).

A insuficiência do quadro normativo brasileiro não resulta, portanto, de uma escolha deliberada de desproteção, mas da incapacidade do processo legislativo de acompanhar o ritmo de implantação das tecnologias. O Smart Sampa foi contratado, implantado e posto em operação em um contexto em que o marco regulatório específico ainda estava sendo discutido no Congresso Nacional. Esse descompasso temporal entre inovação tecnológica e resposta jurídica é, como sustenta Mendes (2026), um padrão estrutural que se reproduz no Brasil e no mundo, e que exige não apenas legislação, mas mecanismos institucionais capazes de avaliar preventivamente os riscos de sistemas de vigilância antes de sua implantação.

5 CONCLUSÃO

Este artigo investigou o impacto da Inteligência Artificial sobre os direitos fundamentais à liberdade e à privacidade, partindo da hipótese de que a insuficiência dos marcos regulatórios vigentes converte a IA em vetor de consolidação de um Panóptico

Digital, uma arquitetura de vigilância onipresente incompatível com os pressupostos de uma sociedade democrática.

Os estudos de caso confirmaram, com consequências juridicamente mensuráveis, que os riscos da vigilância algorítmica não são hipotéticos. O caso Robert Williams demonstrou que o viés estrutural dos dados de treinamento se traduz em restrições indevidas de liberdade que recaem desproporcionalmente sobre minorias raciais. O Smart Sampa evidenciou que, na ausência de regulação específica, o próprio poder público documenta falhas sem dispor de mecanismos efetivos para corrigi-las. Por fim, o caso Clearview AI revelou que infraestruturas de identificação biométrica em escala global podem ser construídas à margem de qualquer consentimento ou base jurídica legítima. Em conjunto, os três casos demonstram um padrão comum: o reconhecimento facial não opera como ferramenta neutra, mas converte o espaço público em ambiente de monitoramento contínuo cujas consequências recaem de forma desproporcional sobre grupos vulneráveis, sem que os indivíduos afetados tenham ciência ou possibilidade de controle.

A análise dos marcos regulatórios confirmou a insuficiência das salvaguardas existentes. O GDPR, robusto instrumento de proteção de dados, revelou-se estruturalmente limitado: o consentimento informado é neutralizado por assimetrias informacionais e *dark patterns*, e a transparência é comprometida pela opacidade técnica inerente a modelos de *machine learning* de alta complexidade. O *AI Act* representa um avanço significativo ao inaugurar proibições específicas para práticas que viabilizaram as violações documentadas neste trabalho. Não obstante, a dependência de autoavaliação pelos próprios fornecedores, a imprecisão técnica das exigências de transparência e as amplas isenções para segurança nacional revelam que mesmo o marco regulatório mais avançado do mundo permanece aquém dos desafios que se propõe a enfrentar.

Da análise conjunta dos casos e dos marcos normativos, emergem três padrões estruturais que definem o desafio regulatório contemporâneo. Em todos os casos examinados, os indivíduos afetados desconheciam que estavam sendo monitorados, identificados ou submetidos a decisões algorítmicas. Essa invisibilidade não constitui falha técnica corrigível, mas característica funcional de sistemas que operam pela dispensabilidade do consentimento. A esse padrão soma-se a insuficiência reativa dos instrumentos jurídicos: o GDPR demonstrou capacidade de impor sanções, mas não de prevenir os danos; o *AI Act* avança nas proibições, mas delega a fiscalização majoritariamente aos próprios regulados. Completa esse quadro a convergência entre vigilância privada e estatal: quando uma empresa constrói um banco de dados biométrico global e o comercializa a agências policiais, as garantias

constitucionais que limitam o poder estatal tornam-se inoperantes, porque o ato originário de vigilância foi praticado por um agente privado.

Esses padrões convergem para confirmar a hipótese central deste trabalho. O Panóptico Digital não é uma metáfora: é a descrição de uma arquitetura de controle já operacional, fragmentada entre atores públicos e privados, desprovida de paredes físicas e alimentada pela própria conduta dos vigiados. Diferente do Panóptico de Bentham, que disciplinava pela incerteza de ser observado, o Panóptico Digital disciplina pela certeza de que tudo é registrado, sem que o titular saiba por quem, para quê e com quais consequências.

No plano normativo, os casos examinados permitem identificar os elementos mínimos de um marco regulatório constitucionalmente adequado para o uso de vigilância biométrica pelo Estado. A autorização legal prévia e específica, ausente no Smart Sampa e exigida pelo art. 5º, LXXIX, da Constituição Federal (Brasil, 1988), é pressuposto inafastável de qualquer sistema que trate dados biométricos em escala populacional. A ela devem somar-se a avaliação de impacto obrigatória antes da implantação, a transparência sobre taxas de erro desagregadas por grupo demográfico e o controle judicial independente sobre os critérios de compartilhamento de dados com outros órgãos. O PL 2.338/2023, em tramitação na Câmara dos Deputados, representa a oportunidade legislativa mais próxima de suprir essa lacuna, mas seu texto aprovado pelo Senado ainda contém exceções amplas para segurança pública que reproduzem, em nível legal, a mesma zona de imunidade regulatória identificada na jurisprudência do TJSP.

A presente investigação não esgota o tema. A atuação da Autoridade Nacional de Proteção de Dados como instância fiscalizadora de sistemas biométricos estatais, a jurisprudência do Supremo Tribunal Federal sobre proporcionalidade em medidas de vigilância e os desdobramentos regulatórios do PL 2.338/2023 constituem eixos de pesquisa que se impõem como agenda necessária. O desafio que se impõe às democracias contemporâneas transcende a dimensão técnica ou jurídica: consiste em delimitar, antes que a arquitetura de vigilância se torne irreversível, quais limites o Direito deve impor ao que a tecnologia é capaz de realizar, assegurando que o desenvolvimento da Inteligência Artificial permaneça subordinado à dignidade da pessoa humana como pressuposto inegociável da ordem jurídica.

REFERÊNCIAS

ACQUISTI, Alessandro; BRANDIMARTE, Laura; LOEWENSTEIN, George. Privacy and human behavior in the age of information. **Science**, Washington, v. 347, n. 6221, p. 509-514, jan. 2015. Disponível em: https://doi.org/10.1126/science.aaa1465. Acesso em: 02 fev. 2026.

ANDREJEVIC, Mark. Automating surveillance. **Surveillance & Society**, [s. l.], v. 17, n. 1/2, p. 7-13, 2019. Disponível em: https://doi.org/10.24908/ss.v17i1/2.12930. Acesso em: 10 jan. 2026.

BENTHAM, Jeremy. **Panopticon; or, The inspection-house.** Londres: T. Payne, 1791. Disponível em: https://archive.org/details/panopticonorins01bentgoog. Acesso em: 2 mar. 2026.

BRASIL. Agência Nacional de Proteção de Dados. **Radar Tecnológico**: biometria e reconhecimento facial. Brasília: ANPD, 2024. Disponível em: https://www.gov.br/anpd/pt-br/centrais-de-conteudo/documentos-tecnicos-orientativos/radar-tecnologico-biometria-e-reconhecimento-facial. Acesso em: 22 fev. 2026.

BRASIL. Constituição (1988). **Constituição da República Federativa do Brasil de 1988.** Brasília, DF: Presidência da República, [1988]. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 10 fev. 2026.

BRASIL. **Lei nº 13.709**, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Diário Oficial da União, Brasília, DF, 15 ago. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 02 fev. 2026.

BRASIL. **Projeto de Lei n.º 2.338, de 2023**: dispõe sobre o uso da Inteligência Artificial. Autor: Sen. Rodrigo Pacheco. Brasília: Senado Federal, 2023. Disponível em: https://www25.senado.leg.br/web/atividade/materias/-/materia/157233. Acesso em: 21 fev. 2026.

CEBREROS, Jannice. Facial recognition technology and wrongful arrests in the digital policing era. **Washington Law Review Online**, Seattle, v. 100, p. 33-64, 2025. Disponível em: https://digitalcommons.law.uw.edu/wlro/vol100/iss2/1. Acesso em: 02 fev. 2026.

COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS (CNIL). **Délibération SAN-2022-019 du 17 octobre 2022**. Paris: CNIL, 2022. Disponível em: https://www.cnil.fr/fr/reconnaissance-faciale-la-cnil-met-en-demeure-clearview-ai-de-cesser-la-reutilisation-de. Acesso em: 02 fev. 2026.

COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS (CNIL). **Délibération SAN-2023-008 du 13 avril 2023**: liquidation d'une astreinte. Paris: CNIL, 2023. Disponível em: https://www.cnil.fr/fr/clearview-ai-la-cnil-liquide-lastreinte-prononcee-lencontre-de-la-societe. Acesso em: 02 fev. 2026.

DUKE, Shaul A. AI and the industrialization of surveillance. **Surveillance & Society**, [s. l.], v. 21, n. 3, p. 282-286, 2023. Disponível em: https://doi.org/10.24908/ss.v21i3.16086. Acesso em: 02 fev. 2026.

ESTADOS UNIDOS DA AMÉRICA. Circuit Court of Cook County, Illinois. **American Civil Liberties Union et al. v. Clearview AI, Inc**. Settlement Agreement. Case No. 20 CH 4353. Chicago, maio 2022. Disponível em: https://casesearch.cookcountyclerkofcourt.org/. Acesso em: 12 fev. 2026.

ESTADOS UNIDOS DA AMÉRICA. United States District Court for the Northern District of Illinois. **In re Clearview AI, Inc**. Consumer Privacy Litigation. MDL No. 2967. Order Granting Final Approval of Class Action Settlement. Chicago, mar. 2025. Disponível em: https://www.ilnd.uscourts.gov/mdl-details.aspx?oPAvB95Dk3B80hctYPQzdQ==. Acesso em: 12 fev. 2026.

ESTADOS UNIDOS DA AMÉRICA. United States District Court for the Eastern District of Michigan, Southern Division. Settlement Agreement. **Williams v. City of Detroit et al. Case** No. 2:21-cv-10827-LJM-DRG, ECF No. 73. Judge: Laurie J. Michelson. Detroit, 28 jun. 2024. Disponível em: https://assets.aclu.org/live/uploads/2024/06/Final-Order-of-Dismissal-and-Settlement-Agreement.pdf. Acesso em: 20 fev. 2026.

EUROPEAN DATA PROTECTION BOARD. **Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement**. Version 2.0. Bruxelas: EDPB, 2023. Disponível em: https://www.edpb.europa.eu/system/files/2023-05/edpb_guidelines_202304_frtlawenforcement_v2_en.pdf. Acesso em: 8 jan. 2026.

FOUCAULT, Michel. **Vigiar e punir**: nascimento da prisão. Tradução de Raquel Ramalhete. 42. ed. Petrópolis: Vozes, 2014.

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI (Garante). **Provvedimento del 10 febbraio 2022** [9751362]. Roma: Garante, 2022. Disponível em: https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9751362. Acesso em: 02 fev. 2026.

GOODMAN, Bryce; FLAXMAN, Seth. European Union Regulations on Algorithmic Decision-Making and a "Right to Explanation". **AI Magazine**, v. 38, n. 3, p. 50-57, 2017. Disponível em: https://onlinelibrary.wiley.com/doi/epdf/10.1609/aimag.v38i3.2741. Acesso em: 10 jan. 2026.

HAN, Byung-Chul. **Psicopolítica**: o neoliberalismo e as novas técnicas de poder. Tradução de Maurício Liesen. Belo Horizonte: Âyiné, 2018.

INFORMATION COMMISSIONER'S OFFICE (ICO). **Monetary Penalty Notice to Clearview AI Inc.** Wilmslow: ICO, 23 maio 2022. Disponível em: https://ico.org.uk/action-weve-taken/enforcement/clearview-ai-inc/. Acesso em: 02 fev. 2026.

INFORMATION COMMISSIONER'S OFFICE (ICO). ICO welcomes Upper Tribunal ruling on Clearview AI. **ICO News**, Wilmslow, 17 out. 2025. Disponível em: https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2025/10/ico-clearview-ai-upper-tribunal/. Acesso em: 21 fev. 2026.

MATHUR, Arunesh; NAOUS, Gunes; VITAK, Jessica; HONG, Jason I.; CHETTY, Marshini. Dark patterns at scale: findings from a crawl of 11K shopping websites.

Proceedings of the ACM on Human-Computer Interaction, New York, v. 3, n. CSCW, art. 81, nov. 2019. Disponível em: https://doi.org/10.1145/3359183. Acesso em: 10 jan. 2026.

MENDES, Laura Schertel; FERNANDES, Elora; ROSAL, Isabela Maria (coord.). **Lei Geral de Proteção de Dados Pessoais comentada**. 1. ed. Rio de Janeiro: Grupo GEN, 2026.

MITTELSTADT, Brent D. *et al.* The ethics of algorithms: mapping the debate. **Big Data & Society**, London, v. 3, n. 2, p. 1-21, dez. 2016. Disponível em: https://doi.org/10.1177/2053951716679679. Acesso em: 02 fev. 2026.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST). **Face Recognition Vendor Test (FRVT) Part 3**: Demographic Effects. GROTHER, Patrick; NGAN, Mei; HANAOKA, Kayee. Gaithersburg: NIST, dez. 2019. (NIST Interagency Report 8280). DOI: https://doi.org/10.6028/NIST.IR.8280. Acesso em: 02 fev. 2026.

NISSENBAUM, Helen. **Privacy in context**: technology, policy, and the integrity of social life. Stanford: Stanford University Press, 2010.

NOUWENS, Midas; LICCARDI, Ilaria; VEALE, Michael; KARGER, David; KAGAL, Lalana. Dark patterns after the GDPR: scraping consent pop-ups and demonstrating their influence. In: CHI CONFERENCE ON HUMAN FACTORS IN COMPUTING SYSTEMS, 2020, Honolulu. **Anais** [...]. New York: ACM, 2020. p. 1-10. Disponível em: https://doi.org/10.1145/3313831.3376321. Acesso em: 10 jan. 2026.

OFFICE OF THE PRIVACY COMMISSIONER OF CANADA (OPC). **Joint investigation of Clearview AI, Inc.** Ottawa: OPC, 2 fev. 2021. Disponível em: https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2021/pipeda-2021-001/. Acesso em: 02 fev. 2026.

OFFICE OF THE PRIVACY COMMISSIONER OF CANADA (OPC). **Provincial authorities issue orders to Clearview AI**. Ottawa: OPC, 15 dez. 2021a. Disponível em: https://www.priv.gc.ca/en/opc-news/news-and-announcements/2021/an_211215/. Acesso em: 02 fev. 2026.

PASQUALE, Frank. **The black box society**: the secret algorithms that control money and information. Cambridge: Harvard University Press, 2015.

QANDEEL, M. Facial recognition technology: regulations, rights and the rule of law. **Frontiers in Big Data**, [s. l.], v. 7, 2024. DOI: 10.3389/fdata.2024.1354659. Disponível em: https://www.frontiersin.org/journals/big-data/articles/10.3389/fdata.2024.1354659/full. Acesso em: 08 fev. 2026.

SÃO PAULO (Estado). Tribunal de Justiça do Estado de São Paulo. 3ª Vara da Fazenda Pública da Capital. **Decisão interlocutória**. Ação Popular n.º 1027876-45.2023.8.26.0053. Juiz: Luis Manuel Fonseca Pires. Julgado em: 18 maio 2023a. Disponível em: https://esaj.tjsp.jus.br/cpopg/show.do?processo.codigo=1H000OSJW0000&processo.foro=53&processo.numero=1027876-45.2023.8.26.0053. Acesso em: 21 fev. 2026.

SÃO PAULO (Estado). Tribunal de Justiça do Estado de São Paulo. 3ª Câmara de Direito Público. **Acórdão**. Agravo de Instrumento n.º 2122169-52.2023.8.26.0000. Rel.: Des.ª Paola Lorena. Julgado em 2 ago. 2023b. Disponível em: https://esaj.tjsp.jus.br/cjsg/getArquivo.do?cdAcordao=17007433&cdForo=0. Acesso em: 21 fev. 2026.

SÃO PAULO (Município). **Programa Smart Sampa atinge meta para 2025 e já soma 40 mil câmeras integradas ao maior sistema de monitoramento da América Latina.** São Paulo: Prefeitura do Município de São Paulo, 2025a. Disponível em: https://prefeitura.sp.gov.br/w/programa-smart-sampa-atinge-meta-para-2025-e-j%C3%A1-soma-40-mil-c%C3%A2meras-integradas-ao-maior-sistema-de-monitoramento-da-am%C3%A9rica-latina. Acesso em: 21 fev. 2026.

SÃO PAULO (Município). Secretaria Municipal de Segurança Urbana. **Relatório de Transparência do Smart Sampa** (nov. 2024 – maio 2025). São Paulo: Prefeitura do Município de São Paulo, 2025b. Disponível em: https://smartsampa.prefeitura.sp.gov.br/relatorio_transparencia_smart_sampa.pdf. Acesso em: 21 fev. 2026.

SOLOVE, Daniel J. **Understanding privacy**. Cambridge: Harvard University Press, 2008.

UNIÃO EUROPEIA. **Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho**, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados. Jornal Oficial da União Europeia, Luxemburgo, L 119, p. 1-88, 4 maio 2016. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A32016R0679. Acesso em: 03 fev. 2026.

UNIÃO EUROPEIA. **Regulamento (UE) 2024/1689 do Parlamento Europeu e do Conselho**, de 13 de junho de 2024, que estabelece regras harmonizadas em matéria de inteligência artificial. Jornal Oficial da União Europeia, Luxemburgo, L, 12 jul. 2024. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=OJ:L_202401689. Acesso em: 15 fev. 2026.

WACHTER, Sandra; MITTELSTADT, Brent; FLORIDI, Luciano. Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation. **International Data Privacy Law**, v. 7, n. 2, p. 76-99, 2017. Disponível em: https://doi.org/10.1093/idpl/ipx005. Acesso em: 03 fev. 2026.

ZUBOFF, Shoshana. Big other: surveillance capitalism and the prospects of an information civilization. **Journal of Information Technology**, [s. l.], v. 30, n. 1, p. 75-89, 2015. Disponível em: https://doi.org/10.1057/jit.2015.5. Acesso em: 10 ago. 2025.

ZUBOFF, Shoshana. **A era do capitalismo de vigilância**: a luta por um futuro humano na nova fronteira do poder. Tradução de George Schlesinger. Rio de Janeiro: Intrínseca, 2021.

ZUCCHETTI FILHO, Pedro. The ViaQuatro and Metropolitan Company of São Paulo FRT cases: implications of different FRT tasks. **International Data Privacy Law**, Oxford, ipaf006, 17 dez. 2025. DOI: https://doi.org/10.1093/idpl/ipaf006. Acesso em: 21 fev. 2026.