A falta de regulamentação do uso da tecnologia de reconhecimento facial na Segurança Pública: impactos nas questões éticas e jurídicas

ANA CECÍLIA ROSÁRIO RIBEIRO

Doutora pela PUCSP
Mestre pela Universidade Autônoma de Lisboa
Especialista pela Universidade Salvador
Promotora de Justiça do MPPI
Professora adjunta da UESPI.

VIVIANE SOUSA BARROS

Bacharel em Direito pela Universidade Estadual do Piauí.

A FALTA DE REGULAMENTAÇÃO DO USO DA TECNOLOGIA DE RECONHECIMENTO FACIAL NA SEGURANÇA PÚBLICA: IMPACTOS NAS QUESTÕES ÉTICAS E JURÍDICAS

THE LACK OF REGULATION ON THE USE OF FACIAL RECOGNITION TECHNOLOGY IN PUBLIC SECURITY: IMPACTS ON ETHICAL AND LEGAL ISSUE

RESUMO

O presente artigo tem como objetivo analisar os impactos éticos e jurídicos proporcionados pelo uso da tecnologia de reconhecimento facial, sobretudo, na segurança pública, ainda que não haja regulamentação no ordenamento brasileiro que legitime seu uso. Em relação às questões éticas urge compreender a forma da aplicação da ferramenta como auxílio no bem coletivo, tendo em vista a carência de regulamentação e de normatização no cenário brasileiro. Ao passo que, tratando-se das questões jurídicas é necessário estabelecer um equilíbrio entre a proteção dos direitos fundamentais individuais dos cidadãos brasileiros violados no uso da tecnologia e o favorecimento no direito público, no que diz respeito à segurança coletiva da sociedade.

Palavras-chave: Reconhecimento facial. Segurança pública. Questões éticas. Questões jurídicas.

ABSTRACT

This article aims to analyze the ethical and legal impacts of the use of facial recognition technology, particularly in criminal justice, even though there is no regulation in Brazilian law that legitimizes its use. Regarding ethical issues, it is urgent to understand how the tool is applied as an aid in public good, given the lack of regulation and standardization in the Brazilian context. On the other hand, in relation to legal issues, it is necessary to establish a balance between the protection of the individual fundamental rights of Brazilian citizens, which may be violated by the use of the technology, and the promotion of public law, particularly regarding the collective security of society.

Keywords: Facial recognition. Public security. Ethical issues. Legal issues.

1. INTRODUÇÃO

A expansão do videomonitoramento urbano tem sido apresentada como uma das principais estratégias de enfrentamento à violência em cidades latino-americanas (ACCESS NOW, 2021; FRANCE 24, 2021)[1].

Essas tecnologias são vistas e utilizadas como aliadas do setor público, na busca de acompanhar a evolução tecnológica no uso do bem coletivo, assumindo um papel central na segurança pública. Nesse contexto, elas podem atuar como um mecanismo de prevenção ao crime, especialmente quando combinadas com processos e práticas eficientes de policiamento, oferecendo suporte em um cenário de recursos limitados.

Entretanto, no cenário brasileiro, há questões a se discutir a respeito da viabilidade da aplicação da tecnologia, tendo em vista a falta de regulamentação consistente a nível federal a respeito do tema, ao passo que, o número de propostas legislativas na Câmara e no Senado é crescente. Dessa maneira, se levanta nesse estudo o embate normativo a respeito da questão ética na aplicabilidade da tecnologia devido à falta de regulamentação.[2]

Dessa forma, faz-se a relação entre o uso da tecnologia no cenário brasileiro e a Teoria da Justiça do filósofo John Finnis, por defender, exatamente, a existência racionalmente cognoscível de uma lei cuja normatividade independe da autoridade política ou da lei positiva, no caso em questão, a lei que positiva o uso da tecnologia de reconhecimento facial (FINNIS, 2007).[3]

Como uma forma de contribuir para a contextualização do assunto, o presente estudo aponta alguns países em que é utilizada a tecnologia, destacando o Reino Unido como um país de referência no que diz respeito à regulamentação da inovação tecnológica.

Ademais, em relação às questões jurídicas, o artigo demonstra que embora a tecnologia seja usada em favor do direito público, especificamente, para proporcionar uma maior segurança pública, os direitos fundamentais individuais são violados na forma da sua aplicabilidade, especialmente, o direito à privacidade e à intimidade, conforme relatório atualizado do projeto O Panótico, do CESeC.[4]

---

[1] FRANCE 24. Gobiernos de América Latina incrementan el uso de videovigilancia. *France24*, 15 ago. 2021. Disponível em: https://www.france24.com/es/programas/revista-digital/20210815-gobiernos-incrementar-videovigilancia-america-latina. Acesso em: 28 jul. 2025.

[2] BRASIL INSTITUTE. **AI regulation still lagging in Brazil**. *Blog do Wilson Center*. Disponível em: https://www.wilsoncenter.org/blog-post/ai-regulation-still-lagging-brazil. Acesso em: 25 jul. 2025

[3] FINNIS, John. Aquinas: Lei natural e direitos naturais. São Leopoldo: Unisinos, 2007.

[4] O **GLOBO**. Reconhecimento facial: 476 milhões de brasileiros estão na mira das câmeras de segurança pública, apontam pesquisa. *O Globo*, 13 dez. 2023. Disponível em:

Assim, os benefícios públicos devem ser amplamente discutidos, assegurando salvaguardas para a proteção de dados e adotando estratégias capazes de mensurar os impactos da tecnologia. Qualquer regulação voltada para o uso e implementação de reconhecimento facial pelo setor público deve seguir princípios claros e transparentes, que garantam a responsabilização das instituições envolvidas.

Portanto, é importante realizar uma análise das principais iniciativas e regulações que têm como objeto a tecnologia do reconhecimento facial, para que assim haja uma comparação ao cenário brasileiro. No artigo em questão, destaca-se o Reino Unido como o país de maior sucesso na implementação da tecnologia de videomonitoramento, com fins de proporcionar a segurança pública, ao tempo em que não viola os direitos fundamentais individuais[5]. Logo, é válida a reflexão e o debate para a utilização responsável de tal sistema.

2. IMPACTOS NAS QUESTÕES ÉTICAS

O uso da ferramenta de tecnologia do reconhecimento facial como uma forma de proporcionar maior segurança pública para os cidadãos brasileiros carece de regulações específicas do tema.

Dessa maneira, urge compreender a legalidade e a eticidade da sua aplicação, através do compilado de legislações que estão associadas ao tema e uma breve relação à Teoria da Justiça do filósofo de John Finnis, já que defende que certos princípios éticos e os direitos humanos podem ser conhecidos por razão prática, sem a necessidade de uma lei que positive.

2.1 Regulamentações acerca do tema

Quando pensa-se em tecnologia de reconhecimento facial, a imagem que geralmente surge é a de uma câmera que identifica rostos em tempo real. Essa aplicação, conhecida como "live detection" (detecção ao vivo), é uma das mais comuns e amplamente utilizada no Brasil, descrita pelo escritor Samuel de Oliveira como:

> A tecnologia de reconhecimento facial funciona mediante o uso de identificação biométrica para mapear características faciais

https://oglobo.globo.com/brasil/noticia/2023/12/13/reconhecimento-facial-476-milhoes-de-brasileiros-estao-na-mira-das-cameras-de-seguranca-publica-aponta-pesquisa.ghtml. Acesso em: 09 out. 2024.

[5] **YOUTH ENDOWMENT FUND.** *Closed-circuit television (CCTV).* 2023. Disponível em: https://youthendowmentfund.org.uk/toolkit/cctv. Acesso em: 28 jul. 2025.

> de uma pessoa presente em uma fotografia ou vídeo, comparando as informações obtidas com um banco de rostos conhecidos para encontrar uma correspondência.(OLIVEIRA, 2021)[6]

No Brasil, ainda não há legislação que regule, especificamente, o uso da tecnologia de reconhecimento facial como medida de segurança pública, apesar de ser uma ferramenta cada vez mais utilizada na segurança pública e até mesmo na justiça criminal, para fins de celeridade processual, tendo em vista que proporciona um auxílio na identificação de suspeitos. Vale ressaltar ainda que no Brasil a implementação dos sistemas pelo setor público tem sido acompanhada por iniciativas de regulação específicas.

De acordo com dados do Panóptico, projeto do Centro de Estudo de Segurança e Cidadania (CESEC), que teve duração de agosto de 2020 a julho de 2022, que monitora a implementação de novas tecnologias na área, cerca de 47,5 milhões de brasileiros estão potencialmente sob vigilância de câmeras de reconhecimento facial na segurança pública. De acordo com os dados da pesquisa, cerca de 23,44% da população brasileira está potencialmente exposta aos sistemas de videomonitoramento com reconhecimento facial, seja em fase de testes ou ativação.[7]

Com isso, observa-se o uso de tecnologia de reconhecimento facial no Brasil sem que haja regulamentação específica sobre o tema. Nesse sentido é o comentário de Thallita Lima, coordenadora da pesquisa do Panóptico, CESEC, em entrevista em 13/12/2023 para o Jornal "O Globo" a respeito do tema:

> [...] A descentralização do uso de reconhecimento facial para fins de segurança pública, com a aquisição por diversos municípios, acende um alerta sobre um possível processo de desresponsabilização do uso dessa tecnologia como política pública de segurança. A pergunta que ecoa quando observamos a multiplicação dos projetos é: qual é o objetivo dessa política? Para quem está sendo desenhada? O que já sabemos é que ela é uma política que não tem se mostrado eficiente e pode automatizar assimetrias sociais e práticas discriminatórias (LIMA, 2023).[8]

---

[6] OLIVEIRA, Samuel. *Sorria, você está sendo filmado!: repensando direitos na era do reconhecimento facial. São Paulo*: Thomson Reuters Brasil, 2021

[7] **CESEC – Centro de Estudos de Segurança e Cidadania.** *O Panóptico: monitor do reconhecimento facial no Brasil*. Rio de Janeiro: CESeC, s.d. Duração do projeto: agosto de 2020 a julho de 2022. Disponível em: https://cesecseguranca.com.br/projeto/o-panoptico-monitor-do-reconhecimento-facial-no-brasil. Acesso em: 25 jul. 2025.

[8] O **GLOBO**. Reconhecimento facial: 476 milhões de brasileiros estão na mira das câmeras de segurança pública, apontam pesquisa. *O Globo*, 13 dez. 2023. Disponível em: https://oglobo.globo.com/brasil/noticia/2023/12/13/reconhecimento-facial-476-milhoes-de-brasileiros-estao-na-mira-das-cameras-de-seguranca-publica-aponta-pesquisa.ghtml. Acesso em: 09 out. 2024.

Contudo, embora não haja regulamentação federal consistente a respeito do tema, vale ressaltar a existência de três propostas legislativas que tramitam hoje na Câmara e no Senado, dentre elas o PL 3.069/2022 e duas leis na esfera estadual, sendo elas: Lei nº 21.737/2015/MG e Lei nº 8.113/2019/AL conforme dados obtidos na pesquisa pelo Instituto Igarapé, instituição que desempenha um papel de *advocacy* para políticas públicas para a superação dos principais desafios globais nas áreas de segurança pública, digital e climática.[9]

O projeto de lei supramencionado possui como objetivo regulamentar o uso de sistemas de reconhecimento facial no âmbito da segurança pública brasileira e, como deve ser regulamentada para sua melhor utilização, afim de asseguras sua máxima eficácia e uso adequado, garantindo a preservação dos direitos fundamentais dos cidadãos, assim como está disposto na justificação:

> Essa ferramenta, como outra qualquer, se corretamente regulamentada, seguramente contribuirá para a redução dos índices de criminalidade em nossa sociedade. Ainda, o Reconhecimento Facial (RF) também pode ser empregado de forma eficaz na busca e localização de pessoas desaparecidas, em especial, crianças, idosos, vulneráveis e/ou pessoas portadores de deficiência ou incapacitação temporária. (PROJETO DE LEI Nº 3.069/2022. Justificação do Projeto de Lei nº 3.069/2022. Câmara dos Deputados, 2022).

Em relação às leis estaduais existentes, apesar de tratar sobre a autorização do uso de reconhecimento facial especificamente em estádio de futebol, na prática, é utilizada para identificar uma ou mais faces dentre as milhares que frequentam estes espaços, sendo o principal objetivo a segurança pública.

Ressalta-se ainda a inconsistência da regulamentação da única norma a respeito do tema a nível federal, que se trata do inciso III do art.4º da Lei Geral de Proteção de Dados (BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais. Art. 4º.). A norma em questão excetua a aplicação da LGPD em questões relacionadas à segurança pública, contudo determina que deverá haver legislação específica para reger estas atividades, o que não ocorre no cenário atual, pois não houve avanços nos projetos de lei.

[9] **IGARAPÉ INSTITUTO**. Regulação do reconhecimento facial no setor público. 2020. Disponível em: https://igarape.org.br/wp-content/uploads/2020/06/2020-06-09-Regula%C3%A7%C3%A3o-do-reconhecimento-facial-no-setor-p%C3%BAblico.pdf. Acesso em: 09 out. 2024.

2.2 Teoria da Justiça de John Finnis

Diante desse cenário, observa-se que a falta de regulamentação que normatize o uso da tecnologia de reconhecimento facial no Brasil proporciona um quadro de insegurança jurídica aos cidadãos. Dessa forma, é importante correlacionar ao pensamento do filósofo australiano John Finnis, que defende a existência, racionalmente cognoscível, de uma lei cuja normatividade independe da autoridade política ou da lei positiva.

A Teoria da Justiça de John Finnis, exposta em sua obra "Natural Law and Natural Rights"[10], defende que a normatividade da lei não é estritamente necessária para a sua legitimidade, isto é, a defesa da filosofia da lei natural, a independência da formalidade das normas estabelecidas para sua legalidade, o que se enquadra no caso em questão.

Na visão do filósofo, a justiça e a moralidade são mais fundamentais do que a mera normatividade da lei, pois acredita que a capacidade da lei de alinhar-se com a razão prática e com os valores humanos universais faz surgir a verdadeira normatividade e contribuir para a realização do bem comum. Assim, critica a visão da legalidade apenas em obediência a regras e normas.

Finnis rejeita, de início, as teorias do contrato social, de que a autoridade se deriva do consentimento dos governados ou de um suposto contrato social. Além disso, rejeita a ideia de que essa autoridade se assente no costume, na herança ou ainda, na transmissão da mesma:

> Consentimento, transmissão, contrato, costume – nada disso é necessário para constituir um estado de coisas que (presumivelmente) justifique alguém alegar constituir e outros reconhecerem sua autoridade para resolver problemas de coordenação, em uma comunidade como um todo, criando regras que tenham autoridade, ou dando ordens ou determinações que tenham autoridade. Pelo contrário, o estado de fatos requerido é este: que, nas circunstâncias, a determinação dessa pessoa, organismo ou configuração de pessoas provavelmente será, em geral, aceita e com base nela se agirá, com a exclusão de qualquer determinação rival e apesar de quaisquer preferências distintas dos indivíduos a respeito do que deveria ser estipulado e feito nos campos relevantes de problemas de coordenação (FINNIS, 2007, pag.242)[11]

Portanto, John Finnis chega a sua definição de direito, derivada dos princípios da razoabilidade prática. Em seu sentido focal, o direito é definido pelo autor como regras feitas, no caso em que comento, a tecnologia tem se mostrado prática e eficaz em diversos países,

[10] FINNIS, John. *Aquinas: Lei natural e direitos naturais*. São Leopoldo: Unisinos, 2007b.

[11] FINNIS, John. Aquinas: Lei natural e direitos naturais. São Leopoldo: Unisinos, 2007, pag.242.

com foco em segurança e praticidade. Assim, para Finnis, o direito é definido como regras feitas:

> [...] de acordo com regras legais reguladoras, por uma autoridade determinada e efetiva (ela própria identificada e, tipicamente, constituída como uma instituição por regras jurídicas) para uma comunidade "completa", e escorada por sanções de acordo com as estipulações guiadas por regras de instituições judicantes, este conjunto de regras e instituições sendo direcionado a resolver de modo razoável qualquer um dos problemas de coordenação da comunidade (e a ratificar, tolerar, regular ou derrogar soluções advindas de outras instituições ou fontes de normas) para o bem comum dessa comunidade, de acordo com uma maneira e uma forma adaptadas a esse bem comum por características de especificidade, minimização de arbitrariedade, e manutenção de uma qualidade de reciprocidade entre os objetos de lei entre si e também em suas relações com as autoridades legítimas (FINNIS, 2007, pag. 270)[12]

Dessa forma, diante do supracitado, apesar das vantagens, no bem coletivo à segurança pública, em se tratando da aplicação da tecnologia de reconhecimento facial na justiça criminal, deve-se ressaltar a importância da sua análise na questão ética, pois está em conformidade com a Teoria da Justiça, tendo em vista o seu uso mesmo com a falta de regulamentação da norma.

3. IMPACTOS NAS QUESTÕES JURÍDICAS

Em relação às questões jurídicas, cumpre ressaltar a necessidade de compreender como o uso da tecnologia de reconhecimento facial viola os direitos individuais fundamentais, ao tempo em que visa favorecer o direito público, especificamente, a segurança pública, favorecendo o bem coletivo.

3.1. Violação dos direitos individuais fundamentais

A coleta e armazenamento de dados biométricos para uso em reconhecimento facial levanta preocupações sobre a invasão de privacidade e a possibilidade de vigilância em massa por parte das autoridades, ou seja, é nítido a violação à dignidade da pessoa humana,

[12] FINNIS, John. Aquinas: Lei natural e direitos naturais. São Leopoldo: Unisinos, 2007, pag.270.

especialmente, em dois direitos fundamentais: a intimidade e a privacidade da pessoa humana, previstos na Constituição República Federativa Brasileira em seu art. 5º, inciso X (BRASIL. Constituição da República Federativa do Brasil de 1988. Art. 5º, X).

Além dos direitos previstos na Constituição Federal, vale ressaltar as normas robustas de garantia e proteção dos direitos individuais previstas na Lei Geral de Proteção de Dados (LGPD), em que trazem um rol extenso de direitos e princípios aplicáveis à coleta e ao tratamento de dados pessoais, inclusive os dados biométricos extraídos do reconhecimento facial, que são considerados dados sensíveis.

O reconhecimento facial funciona graças à utilização de um sistema computadorizado mediante o qual, recorrendo-se a um banco de dados, consegue-se acessar o histórico do indivíduo (profissão, estado civil, antecedentes etc.) que teve a imagem da face capturada pela câmera de vigilância. Essas informações, que se transformam em um algoritmo, um número (tornando-se a identidade biométrica da pessoa), ficam armazenadas para eventual necessidade de comparação futura desses dados com outros.[13]

Dessa maneira, nota-se o uso da tecnologia sem o consentimento explícito do cidadão, criando um estado de vigilância, em que a liberdade de ir e vir é cerceada.

De acordo com o relatório atualizado de 2024 do DHS, os EUA mantêm o uso de reconhecimento facial para segurança e imigração, entretanto mediante reforço de políticas de governança, o que inclui limites no uso, auditorias regulares e comunicação com o público.[14]

Por outro lado, os defensores do banimento nos EUA argumentam que a precisão desses sistemas e os possíveis benefícios setoriais não podem se sobrepor à necessidade de discutir os direitos e a proporcionalidade no uso da tecnologia. Seus argumentos partem da premissa de que a coleta de dados biométricos faciais envolve um alto grau de sensibilidade, configurando-se como uma forma de monitoramento intrusivo, que pode ser realizado sem o conhecimento ou consentimento dos indivíduos, cujos dados estão sendo coletados e processados.[15]

Especificamente na justiça criminal, vale ressaltar um acontecimento em 2019, que se trata de uma parceria realizada entre o governo do estado do Rio de Janeiro e a empresa OI

[13] MOREIRA, Juliano Lucas. Detecção de Componentes Faciais Baseados em Modelos de Cor e Antropometria. 58f. Dissertação (Mestrado em Ciência da Computação) – Faculdade de Informática, Pontifícia Universidade Católica do Rio Grande do Sul, Porto Alegre, 2010, p. 14-15

[14] UNITED STATES. Department of Homeland Security. *2024 update on DHS's use of face recognition and face capture technologies*. Washington, D.C., 16 jan. 2025. Disponível em: https://www.dhs.gov/archive/news/2025/01/16/2024-update-dhss-use-face-recognition-face-capture-technologies. Acesso em: 30 jul. 2025.

[15] HUREL, L.M. Jan./Fev./Mar.(2019). Reconhecimento Facial: Regular, Banir ou Punir. *Insight Inteligência*. Disponível em: https://www.insightinteligencia.com.br/pdfs/84.pdf. Acesso em: 13 nov. 2024

para a implantação do projeto de videomonitoramento no Carnaval de Copacabana, com o objetivo de identificar procurados pela Justiça e carros roubados em tempo real em meio à multidão, coibindo crimes e realizando prisões, por meio do "Termo de Cooperação Técnica", em caráter de prova de conceito, com a duração de 10 dias, compreendendo o período de 1º a 11 de março de 2019.[16]

Contudo, formou-se uma grande polêmica acerca do caso, tendo em vista o histórico da empresa, multada em 2014 pelo Ministério da Justiça em R$3,5 milhões por ter infringido normas de defesa do consumidor ao monitorar o comportamento de clientes na internet e vender essas informações a anunciantes, agências de publicidade e portais na web, com decisão publicada no Diário Oficial da União.

> DESPACHO DO DIRETOR Em 22 de julho de 2014 Processo Administrativo nº 08012.003471/2010-22. Representante: Departamento de Proteção e Defesa do Consumidor ex officio. Re presentado(a): TNL PCS S/A (Oi). Assunto: Prática abusiva. Violação aos princípios da boa-fé e ao direito à privacidade. No-8 - Em acolhimento às razões técnicas consubstanciadas na Nota Técnica nº 137/2014-CGCTPA/DPDC/SENACON, elaborada pela Coordenação-Geral de Consultoria Técnica e Processos Administrativos (fls.), adotando-as inclusive como razão de decidir e, deste modo, considerando a gravidade e a extensão da lesão causada a milhares de consumidores em todo o País, a vantagem auferida e a condição econômica da empresa, nos termos do art. 57 da Lei n. 8.078/90 e art. 25, inciso II e 26, inciso II, do Decreto n. 2.181/97, alterado pelo Decreto n. 7.738/ 2012, aplico à TNL PCS S/A (Oi) a sanção de multa novalor deR$3.500.000,00 (três milhões e quinhentos mil reais), devendo a empresa depositar o valor definitivo da multa em favor do Fundo de Defesa de Direitos Difusos, nos termos da Resolução CFDD n. 16, de 08 demarço de 2005, consoante determina o art. 29, do Decreto n. 2.181/97, alterado pelo Decreto n. 7.738/2012 (Diário Oficial da União, 2014, pág. 43).[17]

Observa-se que durante o processo administrativo foram constatadas violações ao direito à informação, à proteção contra a publicidade enganosa, além do direito à privacidade e à intimidade. Segundo o diretor do Departamento de Proteção e Defesa do Consumidor (DPDC), Amaury Oliva:

[16] Termo de cooperação técnica público no Diário Oficial n° 43 de 28 de fevereiro de 2019
[17] BRASIL. Imprensa Nacional. [DIARIO OFICAL DA UNIÃO]. Disponível em: https://pesquisa.in.gov.br/imprensa/jsp/visualiza/index.jsp?jornal=1&pagina=43&data=23/07/2014. Acesso em: 23 out. 2024.

> A empresa, com o pretexto de melhorar a experiência de navegação, omitiu do consumidor informações essenciais sobre o serviço e suas implicâncias para a privacidade e segurança de dados pessoais. Em nenhum momento o consumidor foi informado de que sua navegação seria monitorada pela empresa e que o seu perfil seria comercializado com empresas de publicidade (OLIVA, 2014).[18]

Portanto, percebe-se uma significativa falta de responsabilidade por parte da empresa OI, em razão da comercialização dos dados dos consumidores, a fim de ofertar publicidade e conteúdo personalizados, sem o devido consentimento dos próprios usuários, o que verifica a violação dos princípios da boa-fé e da transparência.

Nesse sentido, fica nítido a falta de credibilidade proporcionada pela empresa OI, o que torna questionável o resultado da parceria realizada entre o governo do estado do Rio de Janeiro e a empresa OI para a implantação do projeto de videomonitoramento no Carnaval de Copacabana.

Além disso, menciona-se o caso da empresa Via Quatro, concessionária da Linha 4 – Amarela do metrô da capital paulista, que foi condenada, em 10/05/2023, por meio de uma ação civil pública por iniciativa do Instituto Brasileiro de Defesa do Consumidor (IDEC), devido ao uso indevido de imagens de consumidores por meio de reconhecimento facial.

A empresa instalou câmeras em algumas das estações de metrô da capital de São Paulo em abril de 2023 com o intuito de captar e registrar a reação dos passageiros para fins comerciais e publicitários.

Dessa forma, tendo em vista a atividade ilegal, o IDEC ajuizou uma Ação Civil Pública contra a Via Quatro, alegando que a coleta de dados pessoais nas "portas interativas digitais" é ilegal e viola o direito básico dos consumidores à informação, a fim de impedir o uso de qualquer forma de identificação dos usuários da linha, além de requerer indenização pela utilização indevida de imagens e a fixação de dano moral coletivo:

> APELAÇÕES. Ação civil pública. Concessionária da Linha4 do Metrô de São Paulo S.A. (Via Quatro) que opera, por meio das "Portas Interativas Digitais" dos trens da linha de metrô coletando diversos dados e informações dos consumidores usuários. Captação das imagens que eram utilizadas para fins publicitários e comerciais, tendo-se em vista que se buscava detectar as principais características dos indivíduos que circulavam em determinados locais e horários. Ausência de prévia autorização para captação das imagens que demonstra

[18] BRASIL. Ministério da Justiça. Ministério da Justiça multa Oi por monitorar navegação de consumidores na internet. Disponível em: https://www.gov.br/mj/pt-br/assuntos/noticias/ministerio-da-justica-multa-oi-por-monitorar-navegacao-de-consumidores-na-internet. Acesso em: 23 out. 2024.

> conduta muito reprovável caracterizando dano moral coletivo, principalmente considerando o incalculável número de passageiros que transitam pela plataforma da ré todos os dias. Entendimento do C. STJ de que o dano moral coletivo é aferível "in re ipsa", de forma que a sua constatação decorre da apuração da prática ilícita que viole direitos da coletividade, de conteúdo extrapatrimonial. Conquanto inexista fórmula matemática para a apuração do "quantum" devido a título de danos morais coletivos, cediço que deve guardar correspondência com a gravidade do fato, condição de vulnerabilidade dos consumidores usuários e a conduta da causadora do dano, evitando-se, assim, a reiteração da prática ilícita. Necessidade de condenação da ré ao pagamento de indenização no valor de R$ 500.000,00 (quinhentos mil reais), que se mostra suficiente para reparar o dano moral coletivo e prevenir a prática do mesmo tipo de ilícito. RECURSOS DO MINISTÉRIO PÚBLICO DO ESTADO DESÃO PAULO, DO IDEC INSTITUTO BRASILEIRO DEDEFESA AO CONSUMIDOR E DA DEFENSORIAPÚBLICA DO ESTADO DE SÃO PAULO PROVIDOS EMPARTE APENAS PARA MAJORAR O VALOR DO DANOMORAL COLETIVO E NEGADO PROVIMENTO AORECURSO DA CONCESSIONÁRIA DA LINHA 4 DOMETRÔ DE SÃO PAULO S.A. (VIA QUATRO). (TJ – SP Apelação nº 1090663-42.2018.8.26.0100, Relator: Antonio Celso Faria Comarca: São Paulo, Órgão julgador: 8ª Câmara de Direito Público, Data do julgamento: 10/05/2013 e Data de registro:10/05/2023)[19]

O maior problema, segundo o pesquisador do IDEC, Rafael Zanatta, é que o usuário não tem opção para recusar essa coleta de dados:

> Não se trata de impedir as tecnologias de reconhecimento facial, mas sim de adequá-las a dois padrões básicos: adequação de sua utilização e os direitos básicos de consentimento e transparência. Nesse caso, há um cenário de ilegalidade evidente. Primeiro, pois as câmeras não servem para melhoria do transporte ou para segurança, mas sim para análise automática de reações a publicidade. Segundo, pois os usuários do transporte não são informados da coleta de dados e não possuem opção de concordância (ZANATTA, 2019).[20]

Assim, vale mencionar que em relação à exigência do consentimento do cidadão para o uso dos seus dados pessoais, a Lei Geral de Proteção de Dados Pessoais (LGPD), estabeleceu no ordenamento jurídico brasileiro a necessidade de atender às condições previstas no inciso I do Art. 7º para que o tratamento de dados pessoais seja considerado

[19] TJ – SP Apelação nº 1090663-42.2018.8.26.0100, Relator: Antonio Celso Faria Comarca: São Paulo, Órgão julgador: 8ª Câmara de Direito Público, Data do julgamento: 10/05/2013 e Data de registro:10/05/2023

[20] Instituto Brasileiro de Defesa do Consumidor. Justiça impede o uso de câmera que coleta dados do metrô em SP. *Instituto Brasileiro de Defesa do Consumidor*. Disponível em https ://idec.org .br/notícias/j-eu-usar--de -veio-que-copa-sim-fácil-fazer -conheceu-em –sp. Acesso em 10 nov 2024

válido. O artigo determina: “Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses: I - mediante o fornecimento de consentimento pelo titular;” (BRASIL, Lei nº 13.709, 14 de agosto de 2018. *Lei Geral de Proteção de Dados Pessoais,* art. 7º).

A lei especifica que esse consentimento deve ser obtido por escrito ou por outro meio que evidencie a manifestação de vontade do titular, fortalecendo assim a autonomia dos indivíduos em relação à coleta de seus dados pessoais.

O princípio da "autodeterminação informativa" e a importância do consentimento livre e informado são amplamente reconhecidos na doutrina e encontram respaldo no Código de Defesa do Consumidor (Lei 8.078/1990), na Lei do Cadastro Positivo (Lei 12.414/2011) e no Marco Civil da Internet (Lei 12.965/2014), onde são positivados no ordenamento jurídico brasileiro.

A geração de identificadores únicos por meio de algoritmos que tratam dados biométricos, como os utilizados para reconhecimento facial ou reconstrução a partir de dados identificáveis, como no reconhecimento de expressões faciais, viola o novo entendimento sobre a privacidade dos usuários quando estes não consentem com tal prática, especialmente quando o uso se destina a fins comerciais, como no caso supracitado.

Portanto, a implementação da tecnologia ocorre sem a realização de um estudo de impacto adequado e de um debate público abrangente, o que intensifica o risco de violação de direitos e liberdades, especialmente em relação à privacidade e à proteção de dados pessoais, além do agravante pela possível imprecisão e viés nos resultados gerados pelo sistema.

3.2. Benefício do uso da tecnologia no direito público

A implementação da tecnologia de reconhecimento facial tem recebido atenção das autoridades brasileiras, ao tempo em que possui como objetivo principal a garantia da segurança pública. Entretanto, o atual cenário desperta a preocupação do cidadão, devido o potencial de vigilância em massa e as possíveis violações às liberdades individuais. Diante desse cenário, surge a necessidade de uma regulação eficiente que permita tanto o uso responsável da tecnologia quanto a garantia dos direitos individuais.

Ressalta-se que alguns países, na tentativa de acompanhar o desenvolvimento tecnológico e utilizá-lo em favor da coletividade, apresentam diferentes abordagens de autorização do uso, acompanhadas por estratégias regulatórias, como: Reino Unido e França.

Em relação ao emprego de monitoramento por parte de órgãos públicos, o Reino Unido se destaca em razão da experiência na infraestrutura de câmeras de vigilância expandidas pelo país, já que estima-se que o país opere entre 7,5 e 9 milhões de câmeras, o que representa uma densidade de uma câmera para cada 9 ou 10 habitantes (CCTV Services, 2025).[21]

Logo, o histórico de uso de videomonitoramento, combinado com as constantes preocupações da sociedade civil sobre as possíveis violações de direitos civis, levou o país a desenvolver uma legislação robusta sobre o tema ao longo dos anos, além de criar um ecossistema de instituições governamentais responsáveis por monitorar diferentes aspectos do aparato de vigilância estatal.

Esse cenário permitiu ao Reino Unido adotar uma abordagem específica para regulamentar o uso dos sistemas de reconhecimento facial. Embora não exista uma legislação específica dedicada a essa tecnologia, o país elaborou uma série de documentos estratégicos e orientações recomendatórias, que buscam integrar o uso dessa tecnologia no marco jurídico existente, além de estabelecer diretrizes para garantir seu uso responsável por parte dos órgãos públicos.

Assim, cumpre destacar uma pesquisa realizada pelo Instituto Igarapé (09/06/2020): "Regulação do reconhecimento facial no setor público", em que aborda a finalidade e a necessidade do uso da tecnologia no país do Reino Unido. Senão vejamos:

> Como os documentos e legislações analisados justificam a regulação dos sistemas de reconhecimento facial?
> A regulação se justifica para garantir o exercício das atribuições legais das forças policiais que empregam sistemas de reconhecimento facial: proteção da vida e da propriedade; manutenção de ameaças à segurança pública; prevenção e detecção de crimes; persecução criminal e garantia da segurança nacional.
> Quais são os limites impostos aos sistemas de reconhecimento facial?
> Ainda que o rol de finalidades legítimas seja bem amplo, qualquer uso de sistema de reconhecimento facial deve ser considerado necessário para atender uma demanda urgente, proporcional e efetiva. Assim, uma vez implementado, o sistema de reconhecimento facial precisa ter um fim específico e determinado. A mera possibilidade de uso não pode servir como justificativa para tal, bem como o baixo custo ou apoio público. É preciso avaliar se existem meios menos invasivos para atingir a finalidade em questão. Para os casos de vigilância em espaços públicos, não se pode presumir o consentimento da

[21] **CCTV SERVICES.** *How many CCTV cameras are in the UK in 2024?* 11 abr. 2025. Disponível em: https://www.cctv-services.com/how-many-cctv-cameras-are-in-the-uk-in-2024/. Acesso em: 30 jul. 2025.

comunidade, de modo que a instituição que vai operar o sistema deve imprimir esforços para sua obtenção. Mesmo em locais públicos onde não há uma expectativa clara de privacidade dos indivíduos - eliminando assim a necessidade de consentimento - o uso dos sistemas de reconhecimento facial só pode ocorrer quando sua finalidade não puder ser alcançada por outros meios. Todas as justificativas para o emprego em local público precisam ser revistas anualmente.

Quais são os protocolos de uso desses sistemas?

A regulação do Reino Unido ressalta a importância da criação de estruturas administrativas para supervisionar a aplicação de qualquer sistema de vigilância por câmera, incluindo a criação de cadeias de responsabilidade sobre as decisões que determinam o que será gravado, como os dados serão utilizados e para quem podem ser revelados. Todos os procedimentos precisam ser documentados. A regulação também prevê que qualquer protocolo de uso que envolva decisões tomadas com base em informações coletadas por sistemas de reconhecimento facial deve necessariamente envolver intervenção humana, não sendo permitido o emprego de inteligência artificial.

Existe alguma previsão de política de transparência e comunicação aos cidadãos sobre o uso dos sistemas de reconhecimento facial?

A regulação do Reino Unido prevê que, em locais públicos, indivíduos devem ser avisados sobre o emprego de quaisquer câmeras de vigilância, sua justificativa, bem como qual instituição é responsável por sua operação. Contudo, não há necessidade de revelar a localização das câmeras quando a finalidade for a preservação da segurança pública ou a segurança nacional. Também é importante oferecer um canal de acesso para que pessoas que se sintam lesadas pelo emprego das câmeras possam endereçar suas reclamações. O número de reclamações recebidas deverá ser comunicado ao público. Além disso, todos os indivíduos que foram gravados têm direito de acessar suas informações armazenadas pelo sistema, assim como requisitá-las. Os pedidos de requisição devem ser respondidos em até 40 dias. Algumas forças policiais se comprometem a revelar o número total de alertas disparados pelos sistemas de reconhecimento facial, as ações positivas, o número de identificações incorretas, número de prisões e estimativa do total de faces registradas pelas câmeras.

Existe algum incentivo para a utilização de medidas técnicas para a proteção dos dados coletados pelos sistemas de reconhecimento facial?

A regulação do Reino Unido estabelece a necessidade de aplicação de medidas de segurança para evitar acesso e uso não-autorizado dos bancos de dados. Há uma recomendação para que qualquer material gravado seja armazenado de modo a manter a integridade dos dados, garantindo assim a proteção dos direitos individuais de todos os indivíduos filmados pelas câmeras. Para isso, é preciso restringir o acesso à essa informação por parte dos agentes que trabalham na instituição responsável pela coleta e tratamento. Quando possível, recomenda-se também o uso de criptografia e o registro de acesso e uso dos dados, para fins de auditoria. Por fim, há a

> recomendação de que os sistemas sejam fechados, ou seja, não estejam integrados a outros sistemas das forças policiais, ou conectados à Internet.[22]

Dessa maneira, conclui-se que a tecnologia de reconhecimento facial no Reino Unido é implementada de forma que garante a proteção dos cidadãos, ao proporcionar a segurança pública, ao tempo em que não viola os direitos fundamentais individuais. Isso nos mostra que apesar dos benefícios públicos, qualquer regulação desenvolvida especificamente para o uso e a implementação do reconhecimento facial pelo setor público deve ser pautada por princípios claros e transparentes, que possibilitem a responsabilização das instituições envolvidas.

Isso é evidenciado quando a tecnologia é utilizada apenas em último caso, ao esgotar a possibilidade de uso de meio menos invasivo para atingir a finalidade em questão; na responsabilidade da instituição que vai operar o sistema em imprimir esforços para obter o consentimento da comunidade acerca da vigilância em espaço público; na necessidade de aviso aos indivíduos do emprego das câmeras de vigilância, sua justificativa e a instituição responsável pela operação; e, por fim, oferecer um canal de acesso para que pessoas que se sintam lesadas pelo emprego das câmeras possam endereçar suas reclamações além do direito de acessar suas informações armazenadas pelo sistema, assim como requisitá-las.

Assim, observa-se a necessidade de uma regulação dos sistemas de reconhecimento facial e, com base na tendência internacional, de forma cautelosa, pois a capacidade da tecnologia não deve se sobrepor aos riscos oferecidos e já identificados.

Por fim, destaca-se na legislação brasileira a Lei Geral de Proteção de Dados (LGPD), que deixa claro que os princípios da proteção de dados deverão ser observados em absolutamente todos os casos e, mesmo excetuando a aplicação da Lei em questões relacionadas à segurança pública, determina que deverá haver legislação específica para reger estas atividades.

4 CONCLUSÃO

É evidente o quadro de embate entre o direito privado e o direito público no uso da tecnologia de reconhecimento facial, em especial, na segurança pública. Portanto, é essencial

[22] FRANCISCO, Pedro Augusto P.; HUREL, Louise Marie; RIELLI, Mariana Marques. *Regulação do reconhecimento facial no setor público: avaliação de experiências internacionais*. Rio de Janeiro: Instituto Igarapé; Data Privacy Brasil Research, 2020. Disponível em: https://igarape.org.br/wp-content/uploads/2020/06/2020-06-09-Regula%C3%A7%C3%A3o-do-reconhecimento-facial-no-setor-p%C3%BAblico.pdf. Acesso em: 30 jul. 2025.

o equilíbrio e ponderação entre ambos os direitos, a fim de se obter o resultado justo no atual cenário brasileiro.

A regulação do uso de tecnologias emergentes ainda é um desafio complexo, visto que envolve o difícil equilíbrio entre a preservação dos direitos civis e a possibilidade da sociedade usufruir das transformações positivas trazidas pela inovação.

A regulação dessas tecnologias emergentes no Brasil ainda enfrenta desafios significativos, uma vez que a ausência de uma legislação federal clara torna o cenário mais complexo e polêmico. Embora propostas legislativas estejam em trâmite no Congresso Nacional, a necessidade de um marco regulatório robusto e bem ponderado se torna cada vez mais urgente, de modo a assegurar a proteção dos direitos civis e, ao mesmo tempo, possibilitar os benefícios da inovação tecnológica para a sociedade.

REFERÊNCIAS BILIOGRÁFICAS

BRASIL. **Constituição da República Federativa do Brasil de 1988**, promulgada em 5 de outubro de 1988. Art. 5º.

BRASIL. **Imprensa Nacional. [DIARIO OFICAL DA UNIÃO],** pág. 43. Disponível em: https://pesquisa.in.gov.br/imprensa/jsp/visualiza/index.jsp?jornal=1&pagina=43&data=23/07/2014. Acesso em: 23 out. 2024.

BRASIL INSTITUTE. **AI regulation still lagging in Brazil**. *Blog do Wilson Center*. Disponível em: https://www.wilsoncenter.org/blog-post/ai-regulation-still-lagging-brazil. Acesso em: 25 jul. 2025

BRASIL**. Lei nº 13.709. Lei Geral de Proteção de Dados Pessoais**, promulgada em 14 de agosto de 2018. Art. 4º.

BRASIL. **Ministério da Justiça. Ministério da Justiça multa Oi por monitorar navegação de consumidores na internet.** Disponível em: https://www.gov.br/mj/pt-br/assuntos/noticias/ministerio-da-justica-multa-oi-por-monitorar-navegacao-de-consumidores-na-internet. Acesso em: 23 out. 2024.

CCTV SERVICES. **How many CCTV cameras are in the UK in 2024?** 11 abr. 2025. Disponível em: https://www.cctv-services.com/how-many-cctv-cameras-are-in-the-uk-in-2024/. Acesso em: 30 jul. 2025.

CESEC – Centro de Estudos de Segurança e Cidadania. **O Panóptico: monitor do reconhecimento facial no Brasil.** Rio de Janeiro: CESeC, s.d. Duração do projeto: agosto de 2020 a julho de 2022 Disponível em: https://cesecseguranca.com.br/projeto/o-panoptico-monitor-do-reconhecimento-facial-no-brasil. Acesso em: 25 jul. 2025.

FRANCE 24. **Gobiernos de América Latina incrementan el uso de videovigilancia**. *France24*, 15 ago. 2021. Disponível em: https://www.france24.com/es/programas/revista-digital/20210815-gobiernos-incrementar-videovigilancia-america-latina. Acesso em: 28 jul. 2025.

FRANCISCO, Pedro Augusto P.; HUREL, Louise Marie; RIELLI, Mariana Marques. **Regulação do reconhecimento facial no setor público: avaliação de experiências internacionais.** Rio de Janeiro: Instituto Igarapé; Data Privacy Brasil Research, 2020. Disponível em: https://igarape.org.br/wp-content/uploads/2020/06/2020-06-09-Regula%C3%A7%C3%A3o-do-reconhecimento-facial-no-setor-p%C3%BAblico.pdf. Acesso em: 30 jul. 2025.

FINNIS, John. Aquinas**: Lei natural e direitos naturais**. São Leopoldo: Unisinos, 2007b.

FINNIS, J. Aquinas**: Moral, Political and Legal Theory.** Oxford: Oxford University Press, 1998.

FINNIS, J. Aquinas. **Fundamentos de ética**. Rio de Janeiro: Elsevier, 2012.

HUREL, L.M. Jan./Fev./Mar.(2019). **Reconhecimento Facial: Regular, Banir ou Punir. Insight Inteligência.** Disponível em: https://www.insightinteligencia.com.br/pdfs/84.pdf. Acesso em: 13 nov. 2024.

IGARAPÉ INSTITUTO. **Regulação do reconhecimento facial no setor público**. 2020. Disponível em: https://igarape.org.br/wp-content/uploads/2020/06/2020-06-09-Regula%C3%A7%C3%A3o-do-reconhecimento-facial-no-setor-p%C3%BAblico.pdf. Acesso em: 09 out. 2024.

Instituto Brasileiro de Defesa do Consumidor. **Justiça impede o uso de câmera que coleta dados do metrô em SP**. Instituto Brasileiro de Defesa do Consumidor. Disponível em https ://idec.org .br/notícias/j-eu-usar--de -veio-que-copa-sim-fácil-fazer -conheceu-em –sp. Acesso em 10 nov 2024.

MOREIRA, Juliano Lucas. **Detecção de Componentes Faciais Baseados em Modelos de Cor e Antropometria**. 58f. Dissertação (Mestrado em Ciência da Computação) – Faculdade de Informática, Pontifícia Universidade Católica do Rio Grande do Sul, Porto Alegre, 2010, p. 14-15.

O GLOBO. **Reconhecimento facial: 476 milhões de brasileiros estão na mira das câmeras de segurança pública, apontam pesquisa.** O Globo, 13 dez. 2023. Disponível em: https://oglobo.globo.com/brasil/noticia/2023/12/13/reconhecimento-facial-476-milhoes-de-brasileiros-estao-na-mira-das-cameras-de-seguranca-publica-aponta-pesquisa.ghtml. Acesso em: 09 out. 2024.

OLIVEIRA, Samuel. **Sorria, você está sendo filmado!: repensando direitos na era do reconhecimento facial.** São Paulo: Thomson Reuters Brasil, 2021.

Termo de cooperação técnica público no Diário Oficial n° 43 de 28 de fevereiro de 2019.

TJ – SP Apelação nº 1090663-42.2018.8.26.0100, Relator: Antonio Celso Faria Comarca: São Paulo, Órgão julgador: 8ª Câmara de Direito Público, Data do julgamento: 10/05/2013 e Data de registro:10/05/2023.

UNITED STATES**. Department of Homeland Security. 2024 update on DHS's use of face recognition and face capture technologies**. Washington, D.C., 16 jan. 2025. Disponível em: https://www.dhs.gov/archive/news/2025/01/16/2024-update-dhss-use-face-recognition-face-capture-technologies. Acesso em: 30 jul. 2025.

YOUTH ENDOWMENT FUND**. Closed-circuit television (CCTV).** 2023. Disponível em: https://youthendowmentfund.org.uk/toolkit/cctv. Acesso em: 28 jul. 2025.