Diário Oficial
Estado de São Paulo

Poder Legislativo
Palácio Nove de Julho
Av. Pedro Álvares Cabral, 201
Ibirapuera - CEP: 04097-900
Fone: (011) 3886-6122

Diário da Assembléia Legislativa –

Nº 110 - DOE – 23/06/2022 - p.3

**PROJETO DE LEI Nº 385, DE 2022**

Dispõe sobre a restrição do uso de tecnologias de reconhecimento facial pelo Poder Público no Estado de São Paulo.

A ASSEMBLEIA LEGISLATIVA DO ESTADO DE SÃO PAULO DECRETA:

Artigo 1º Esta Lei dispõe sobre restrições do uso de tecnologias de reconhecimento facial pelo Poder Público no Estado de São Paulo

Artigo 2º Para os fins desta Lei, considera-se:

I. Reconhecimento facial: processamento automatizado ou semi-automatizado de imagens que contenham faces de indivíduos, com o objetivo de identificar, verificar ou categorizar esses indivíduos;

II. Tecnologia de reconhecimento facial: qualquer programa de computador que realiza o reconhecimento facial;

III. Controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais, conforme disposto na Lei Federal nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais - LGPD);

Artigo 3º Fica vedado, nos termos desta Lei, ao Poder Público no Estado de São Paulo:

I. Obter, adquirir, reter, vender, possuir, receber, solicitar, acessar, desenvolver, aprimorar ou utilizar tecnologias de reconhecimento facial ou informações derivadas de uma tecnologia de reconhecimento facial;

II. Celebrar contrato com terceiro com a finalidade ou objetivo de obter, adquirir, reter, vender, possuir, receber, solicitar, acessar, desenvolver, aprimorar ou utilizar tecnologias de reconhecimento facial, informações derivadas de uma tecnologia de reconhecimento facial ou manter acesso à tecnologia de reconhecimento facial;

III. Celebrar contrato com terceiro que o auxilie no desenvolvimento, melhoria ou expansão das capacidades da tecnologia de reconhecimento facial ou forneça ao terceiro acesso a informações que o auxiliem a fazer isso;

IV. Instruir pessoa jurídica de direito público ou privado a adquirir ou usar tecnologias de reconhecimento facial em seu nome;

V. Permitir que pessoa jurídica de direito público ou privado use tecnologias de reconhecimento facial em áreas urbanas, rurais ou mistas de sua circunscrição;

VI. Implantar ou operacionalizar tecnologias de reconhecimento facial nos espaços públicos e privados do Estado de São Paulo;

§1º A vedação prevista no caput aplica-se ao Poder Público do Estado de São Paulo, em sua administração direta e indireta, bem como às concessionárias e permissionárias de serviços públicos.

§2º A vedação prevista no caput aplica-se a tecnologias de reconhecimento facial adquiridas por qualquer meio, com ou sem troca de dinheiro ou outra contraprestação.

Artigo 4º Em sendo dada ciência ao Poder Público do Estado de São Paulo sobre a aquisição ou uso inadvertido ou não intencional de tecnologias de reconhecimento facial ou informações derivadas de tecnologia de reconhecimento facial, as tecnologias e informações não deverão ser mais utilizadas e deverão ser excluídas no prazo de até 10 dias da descoberta do fato, sob as penas previstas nos termos da Lei.

Parágrafo único. O controlador deverá registrar o recebimento, acesso ou uso de tais informações e deve identificar as medidas tomadas pelo Poder Público para evitar a transmissão ou uso de quaisquer informações obtidas inadvertidamente ou não intencionalmente através do uso da tecnologia de reconhecimento facial.

Artigo 5º Após a entrada em vigor desta Lei, as tecnologias de reconhecimento facial previamente implementadas e informações derivadas destas tecnologias não deverão ser mais utilizadas e deverão ser excluídas no prazo de até 10 dias da descoberta do fato.

Parágrafo único. O controlador deverá registrar o recebimento, acesso ou uso de tais informações e deve identificar as medidas tomadas pelo Poder Público para a exclusão dessas tecnologias e informações.

Artigo 6º Esta Lei não se aplica ao dispositivo eletrônico pessoal, tais como telefone celular ou tablet, de propriedade do Estado de São Paulo, que realiza reconhecimento facial com o único propósito de autenticação do usuário pertencente a seu quadro de servidores.

Artigo 7º As vedações de que trata esta Lei não se aplicam ao uso da tecnologia de reconhecimento facial exclusivamente utilizada para pesquisas científicas realizadas por institutos, centros de pesquisa ou universidades.

Artigo 8º O descumprimento ao disposto no art. 3º desta Lei poderá ser punido com sanção de multa no valor de São Paulo a ser aplicada na pessoa do agente, sem prejuízo de outras penalidades previstas em legislação específica na esfera penal, cível e administrativa.

Parágrafo único. A receita arrecadada com a multa, da qual trata o caput deste artigo, será revertida para o Fundo Estadual de São Paulo.

Artigo 9º Esta lei deverá ser regulamentada no prazo máximo de 120 (cento e vinte) dias de sua publicação.

Parágrafo único. O processo de regulamentação de que trata o caput deverá abranger a realização de consulta e audiência públicas e oitiva dos conselhos estaduais vinculados às Secretarias de Segurança Pública e de Justiça e Cidadania de São Paulo, no âmbito de suas competências.

Artigo 10 As despesas decorrentes da execução desta Lei correrão por conta de dotações orçamentárias próprias, suplementadas, se necessário.

Artigo 11 Esta Lei entra em vigor na data de sua publicação.

**JUSTIFICATIVA**

Este projeto prevê a restrição do uso de tecnologias de reconhecimento facial pelo Poder Público no Estado de São Paulo.

Primeiramente, é necessário identificar como funciona a tecnologia de reconhecimento facial. Partindo do tratamento de informações sobre o rosto de uma pessoa, a tecnologia do reconhecimento facial primeiro coleta a imagem do rosto, logo depois, o sistema identifica métricas específicas da pessoa, como a distância entre os olhos, largura do queixo e o comprimento da boca. Por fim, com essas informações (dados biométricos), é calculada uma espécie de assinatura facial. Esta assinatura é comparada com outras já armazenadas em um banco de dados e, quando as assinaturas faciais são compatíveis, em teoria, seria possível identificar um sujeito de forma automatizada.

Ocorre que no processo de identificação das métricas faciais da pessoa, os algoritmos podem cometer erros devido a expressões faciais, rosto mal iluminado, envelhecimento, transições de gênero, entre outros. Além disso, boa parte desses algoritmos são treinados a reconhecer rostos a partir de bancos de dados em que não há pessoas racializadas, e nem mesmo mulheres, de forma significativa, resultando em maior dificuldade para algoritmo criar uma assinatura facial acurada para essas populações. Em estudo que marca o campo, a pesquisadora do MIT, Joy Buolamwini, e a cientista de dados Timnit Gebru, se dedicaram a apontar o viés de gênero e raça em diferentes sistemas de reconhecimento facial no projeto Gender Shades. Em um teste preliminar, avaliou-se que os sistemas da Microsoft, Facebook e IBM, tendo em vista que alguns deles eram vendidos para governos. E os resultados foram: esses sistemas dão respostas de forma acurada quando os sujeitos são homens brancos, mas a proporção de acertos cai no caso de homens negros e é menor ainda no caso de mulheres negras. Ou seja, mulheres negras ficam mais sujeitas a falsos positivos. Na análise de erro da Microsoft, por exemplo, a pesquisadora demonstra que 93,6% das imagens que tiveram o gênero equivocado eram de rostos negros.

A grande possibilidade de erros, principalmente para a população negra, custa na restrição de direitos de muitas pessoas, como aconteceu no Rio de Janeiro, quando uma mulher foi detida no segundo dia de uso dessa tecnologia. Os sistemas presentes no mercado possuem uma precisão que varia entre 75,8% e 87,5% quando aplicadas em população racializada, o que tem resultados em diversos erros com consequências graves.

Um estudo produzido pela Rede de Observatórios da Segurança que levantou 151 casos de prisões com o uso de reconhecimento facial em que 90% dos casos eram de pessoas negras, presas por crimes com baixo potencial ofensivo como tráfico de pequenas quantidades de drogas e furtos.

Outra pesquisa mais recente, feita por uma das maiores empresas de reconhecimento facial, a francesa Idemia, afirma que a tecnologia possuía maior probabilidade de identificar de forma incorreta mulheres negras em relação às mulheres brancas ou homens brancos em relação a homens negros. Entre mulheres brancas a taxa de erro foi de 1 para cada 10 mil, no de mulheres negras, a taxa foi de 1 para 1 mil, ou seja, 10 vezes mais chance de erro.

Na cidade de São Francisco (coração do Vale do Silício nos Estados Unidos), o uso da tecnologia de reconhecimento facial nos espaços públicos foi banido em razão do alto potencial de uso abusivo e de instauração de um estado de vigilância opressiva e massiva. A tendência de banimento, considerando que tecnologias podem criar ou perpetuar opressões já existentes na sociedade e que as tecnologias de reconhecimento facial têm mostrado pouca acurácia na identificação de pessoas negras e mulheres, foi também seguida nas cidades de Portland, Mineápolis, Cambridge, Oakland, Nova Orleans e dezenas de outros municípios norte-americanos.

Na Europa, entidades do poder público, como a Comissão Europeia, o Conselho da Europa e Autoridades de Proteção de Dados, têm exigido uma aplicação imediata do princípio da precaução e recomendam uma proibição geral de qualquer utilização de tecnologias de reconhecimento facial em espaços acessíveis ao público, em qualquer contexto. Em março de 2021, a Autoridade Europeia de Proteção de Dados emitiu um parecer pedindo o banimento de tecnologias de reconhecimento facial em todo o bloco europeu. Ainda no contexto europeu, a nova coalizão que

compõe o governo alemão pediu por um banimento amplo do uso de tecnologias de biometria facial no continente e, mais recentemente, a Itália proibiu o uso de reconhecimento facial em espaços públicos e abertos ao público.

A IBM, uma das maiores empresas de tecnologia do mundo, anunciou que deixaria de investir em tecnologias de reconhecimento facial, já que, segundo a empresa, esse instrumento estaria sendo utilizado para controle social e opressão pelas forças policiais. Em junho de 2020, a Amazon também proibiu que utilizem tecnologias de reconhecimento facial da empresa para finalidades policiais.

Seguindo esse posicionamento, a Microsoft tornou-se a terceira empresa de tecnologia a indicar que não venderá suas soluções em tecnologias de reconhecimento facial para a polícia estadunidense. Em 2021, foi a vez do Facebook anunciar o fim de sua ferramenta de reconhecimento facial que identificava automaticamente os usuários em fotos e vídeos. Mark Zuckerberg se comprometeu ainda a deletar todos os registros feitos até agora em sua plataforma.

Diversas organizações ao redor do mundo já se posicionaram pelo impedimento de utilização desse tipo de tecnologia, como o manifesto capitaneado pela Access Now, Anistia Internacional, European Digital Rights (EDRi), Human Rights Watch, Internet Freedom Foundation (IFF) e o Instituto Brasileiro de Defesa do Consumidor (Idec) que reuniu organizações de todo mundo, incluindo do Brasil, que se posicionaram pelo banimento de tecnologias biométricas em espaços públicos.

Insegurança jurídica e ineficiência no gasto público:

Cabe ressaltar sobre a insegurança jurídica e ineficiência no gasto público que a utilização de tecnologia de reconhecimento facial acarreta. Primeiramente, a implementação dessa tecnologia requer um enorme grupo de funcionários para a sua operação, incluindo os operadores do sistema, os policiais militares que fazem a abordagem dos denominados “suspeitos” de terem mandados abertos em seus nomes, dentre outros. Neste sentido, tendo em vista o já sabido nível de erro que esses sistemas possuem, o uso dessas tecnologias significa redução da eficiência, uma vez que gera trabalho extra na abordagem de cada caso de falso positivo pelos agentes públicos. Por exemplo, em 2019, nos quatro dias da Micareta de Feira de Santana, na Bahia, o sistema de videomonitoramento capturou os rostos de mais de 1,3 milhões de pessoas, gerando 903 alertas, o que resultou no cumprimento de 18 mandados e na prisão de 15 pessoas, ou seja, de todos os alertas emitidos, mais de 96% não resultaram em nada.

Já em relação aos gastos financeiros, Estados Federados e Municípios têm adquirido sistemas de reconhecimento facial por dezenas de milhares de reais ao mesmo tempo em que outras áreas importantes para os cidadãos, como saneamento básico, educação e saúde se encontram sucateadas e sem o devido financiamento. Como exemplo, o Estado da Bahia anunciou a expansão do sistema de reconhecimento facial para mais de 70 municípios do interior, com o gasto de 665 milhões de reais. Em algumas cidades que ganharão as câmeras faltam escolas, hospitais, serviços de acesso à justiça, etc.

Em 2018, a Justiça de São Paulo suspendeu o uso de tecnologias similares no transporte público, determinando que uma concessionária do Metrô da capital paulista cessasse a coleta de dados de som e imagem biométrica dos usuários, com a justificativa de que o tratamento de dados dessa forma atentaria contra o direito constitucional à intimidade e à vida privada, bem como os direitos dos consumidores. Nesse mesmo caso, a concessionária foi condenada pela Justiça a pagar R$100 mil como multa por captar imagens dos passageiros sem prévia autorização. Mais recentemente, em outra decisão sobre um edital de licitação para compra de câmeras de reconhecimento facial, o Poder Judiciário determinou que o Metrô de São Paulo prestasse esclarecimentos sobre o sistema e suspendesse o uso de tecnologia de reconhecimento facial.

Assim, percebe-se que a insegurança jurídica tende a crescer exponencialmente caso tecnologias de reconhecimento facial sejam empregadas. Eventuais ações judiciais contra o uso de reconhecimento facial podem levar à suspensão de editais de licitação, gastos com custas processuais e, em casos mais extremos, ao pagamento de indenizações e multas por erros decorrentes de falsos positivos em reconhecimento facial ou vazamento de dados sensíveis.

Direitos fundamentais:

É preciso também reforçar sobre a violação de direitos fundamentais, já que o uso de tecnologias de reconhecimento facial afronta a dignidade da pessoa humana, a privacidade, o direito à proteção de dados pessoais, a liberdade de ir e vir, e a inviolabilidade da honra e da imagem das pessoas. O uso desse tipo de tecnologia também ameaça o princípio da presunção de inocência, já que trata todo indivíduo como potencial suspeito a ser monitorado e identificado pelo Estado. Trata-se, ainda, de violação ao direito de proteção de dados pessoais, reconhecido como direito fundamental autônomo pelo STF em maio de 2020 e incluído na Constituição Federal como direito fundamental dos cidadãos, pela Emenda Constitucional nº 115, de 2022.

A vigilância em larga escala ocorre de forma irrestrita, sem definição prévia de um alvo específico e muitas vezes ininterruptamente. Segundo diretrizes emitidas pela Alta Comissária para Direitos Humanos da ONU e pelo Relator Especial da ONU para o Direito à Privacidade, é preciso impor limites ao uso de tecnologias de reconhecimento facial. O uso da tecnologia ainda tende a causar um “efeito inibidor”: o receio de estar sendo vigiado ou rastreado restringe a participação das pessoas em assembleias e no espaço cívico, impedindo-as de se expressar sem constrangimento.

Racismo e Transfobia:

Necessário se faz considerar o racismo existente na implementação destas tecnologias, em razão de diferenças significativas quanto à (falta de) acurácia de sistemas de reconhecimento facial na avaliação de rostos de pessoas não brancas, importa destacar que soluções em tecnologias de reconhecimento facial não são neutras e refletem o racismo pré-existente na sociedade. Assim, pensando na sua aplicação em contextos de segurança que remetem ao seletivismo penal e ao aprimoramento de políticas criminais com efeitos nocivamente racializados, trata-se de um risco grave e já observado em diversas situações que representam segurança para algumas pessoas e repressão para outras.

A transfobia é outro elemento a ser observado, pois a imposição de critérios binários na sociedade, ou seja, de classificação entre homem e mulher, promove classificações que reforçam a exclusão e o estigma de pessoas transgênero e não-binárias. Isso não seria diferente no que diz respeito aos sistemas de reconhecimento facial, os quais reiteradamente negam visibilização a identidades divergentes - conflitando com a auto identificação de gênero, acirrando violências e reiterando o cerceamento de direitos às pessoas transexuais e não-binárias. No Brasil, temos diversos casos documentados de falsos negativos, ou seja, do sistema não reconhecer que a pessoa era ela mesma. Foi o caso da estudante Maria Eduarda, no Distrito Federal, que teve seu passe bloqueado no DFtrans. Dona do cartão, mulher negra e trans, mesmo depois de entrar com recurso pedindo a suspensão do bloqueio, continuou sem passe e sem poder exercer um direito que lhe garantia acesso à educação.

Crianças e adolescentes:

Quanto à violação dos direitos de crianças e adolescentes, podemos frisar que a privacidade da população infanto-juvenil é garantida pelo ordenamento jurídico brasileiro tanto no que diz respeito ao direito de imagem quanto ao tratamento de seus dados pessoais em prol do seu melhor interesse, sendo necessário o consentimento específico por seu responsável para tanto. Pela impossibilidade de sistemas de tecnologias de reconhecimento facial

serem utilizados em espaços públicos sem coletar dados de menores e incapazes, eles representam uma ameaça aos direitos de indivíduos dessa faixa etária.

Reconhecimento facial como medida ineficaz, inadequada e onerosa:

Isto posto, ante a impossibilidade de se atingir o fim que pretende, o uso de tecnologias de reconhecimento facial ofende ao postulado da proporcionalidade. O primeiro passo para verificar a obediência ao princípio é a adequação de uma medida, isto é, as possibilidades de ela levar à realização da sua finalidade. A instalação de um sistema de reconhecimento facial é justificativa inadequada para proteção da segurança e persecução de foragidos. Conforme já visto, inúmeros são os casos de falsos positivos que provocaram erros na atividade de fiscalização estatal - tanto que internacionalmente tal medida é coibida.

Desta maneira, o uso de tecnologias de reconhecimento facial mostra-se meio inadequado e ineficaz. Por sua vez, a utilização desnecessária de recursos onera o erário público além de prejudicar a fiscalização e, portanto, atenta contra o interesse público.

Assim, resta demonstrado que o reconhecimento facial tem falhas técnicas significativas em suas formas atuais, incluindo sistemas que refletem as contradições discriminatórias presentes na sociedade, e são menos acurados para pessoas com tons de pele mais escuros. Entretanto, as melhorias técnicas desses sistemas não evitarão a ameaça que representam aos nossos direitos humanos.

Essas tecnologias representam uma ameaça aos nossos direitos. Primeiramente, os dados de treinamento - o banco de dados de rostos com o qual os dados de entrada são comparados e os dados biométricos tratados por esses sistemas - são geralmente obtidos sem o conhecimento, consentimento ou escolha genuinamente livre daqueles que estão incluídos neles, o que significa que essas tecnologias incentivam a vigilância em massa e discriminatória desde sua concepção.

Em segundo lugar, enquanto as pessoas em espaços acessíveis ao público puderem ser instantaneamente identificadas, destacadas ou rastreadas, seus direitos humanos serão minados. Até a ideia de que essas tecnologias poderiam estar em operação em espaços acessíveis ao público cria um efeito inibitório que mina a capacidade das pessoas de exercerem seus direitos, especialmente o direito constitucional à liberdade de expressão, reunião e manifestação.

Por tudo exposto, resta evidente que tal tecnologia não pode ser indiscriminadamente utilizada e deve ser impedida de ser implementada nos espaços públicos do território do Estado de São Paulo, assim como seu uso deve ser banido imediatamente.

Desta forma, resta justificada a presente propositura e espero contar com o apoio dos nobres colegas desta Casa, para a aprovação do presente Projeto de Lei.

Sala das Sessões, em 22/6/2022.

a) Leci Brandão - PC do B

a) Isa Penna - PC do B

a) Érika Malunguinho - PSOL