

## Nota Técnica | Pelo veto do Projeto de Lei nº 865/19

Em consideração à aprovação do **Projeto de Lei nº 865/19**, que dispõe sobre a instalação de **tecnologia de reconhecimento facial (TRF)** nas estações **do Metrô e da CPTM**, cuja aprovação contou com exígua discussão social sobre o tema, o Laboratório de Políticas Públicas e Internet (LAPIN), a Access Now, o Instituto de Tecnologia e Sociedade do Rio (ITS Rio) e as entidades que abaixo subscrevem vêm, por meio desta Nota Técnica, **instar pelo veto total ao PL 865/2019 SP, por ser inconstitucional e contrário ao interesse público, pelas razões abaixo.**

### 1. Breve Síntese do PL nº 865/19

Proposto em 2019 pelo Deputado Estadual Sr. Rodrigo Gambale (PSL), o Projeto de Lei nº 865 inicialmente dispunha sobre a **instalação obrigatória de câmeras equipadas com TRF** em todas as **estações do Metrô e da CPTM**, bem como no interior dos vagões. O Projeto trazia a justificativa de preservação da segurança, incluindo a previsão de **parcerias com órgãos de segurança pública** para a eventual localização de criminosos foragidos.

Em análise pela Comissão de Constituição e Justiça da Assembleia Estadual, foi identificada inconstitucionalidade formal por contrariedade à competência privativa do Executivo em direcionar atos da Administração Pública estadual. Em razão disso, o projeto foi aprovado na Sessão Parlamentar de 10 de fevereiro de 2021 em regime de urgência, na redação de um substitutivo que não mais obrigava, mas autorizava o Poder Executivo a instalar câmeras com TRF nas estações.

### 2. Na contramão de banimentos e moratórias

Mesmo que a implementação de TRF já se dê em diversas unidades federativas brasileiras, em um contexto de ausência de disposição legal específica sobre o tema, importa destacar recomendações de especialistas que alertam para **riscos éticos e de**

**vigilância massiva, além de violações de direitos fundamentais e falta de mecanismos que demonstrem a eficiência da tecnologia.**

### **a. Posicionamento internacional**

Especialmente nos Estados Unidos, há uma tendência ao banimento do uso de tecnologias de reconhecimento facial. Na cidade de São Francisco, o uso de TRF foi banido em razão do alto potencial de uso abusivo e de instauração de um estado de vigilância opressiva e massiva. A cidade de Portland, em Oregon, por sua vez, banuiu o uso de TRF diante do movimento *Black Lives Matter*<sup>1</sup>, oportunidade em que evidenciou a existência de um viés prejudicial a pessoas negras decorrente dessa tecnologia.

Também nos EUA, o Conselho Municipal de Mineápolis decidiu por seu banimento no contexto da Administração Pública em fevereiro de 2021, considerando que tecnologias podem criar ou perpetuar opressões já existentes na sociedade e que as TRF têm mostrado pouca acurácia na identificação de pessoas negras e mulheres. Isso foi feito com vistas à prevenção de discriminações e como forma de promover privacidade e transparência<sup>2</sup>. A tendência de banir a TRF foi também seguida nas cidades de Berkeley, Jackson, Springfield e outras<sup>3</sup>.

### **b. Posicionamentos no Setor Privado**

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<sup>4</sup>. A **Amazon** também proibiu que utilizem a TRF da empresa por um ano para

---

<sup>1</sup> O movimento Vidas Negras Importam é uma campanha contra a violência direcionada às pessoas negras. Para mais informações, acesse: <https://www.uol.com.br/universa/noticias/redacao/2020/06/03/black-lives-matter-conheca-o-movimento-fundado-por-tres-mulheres.htm>

<sup>2</sup> ORDINANCE. Amending Title 2, Chapter 41 of the Minneapolis Code of Ordinances relating to Administration: Information Governance. 2021. Disponível em: <https://lms.minneapolismn.gov/Download/File/4860/Facial%20Recognition%20Ordinance%2001.21.2021.pdf>. Acesso em: 1 mar. 2021.

<sup>3</sup> BAN FACIAL RECOGNITION. Interactive Map. [S.l.], 2020. Disponível em: <https://www.banfacialrecognition.com/map/>. Acesso em: 05 dez. 2020.

<sup>4</sup> IBM. IBM CEO's Letter to Congress on Racial Justice Reform. 2020. Disponível em: <https://www.ibm.com/blogs/policy/facial-recognition-sunset-racial-justice-reforms/>. Acesso em: 05 set. 2020.

as finalidades policiais a fim de que, durante esse período, sejam elaboradas regulamentações que assegurem o uso ético da tecnologia<sup>5</sup>. Seguindo esse posicionamento, a **Microsoft** tornou-se a terceira empresa de tecnologia a indicar que não venderá suas soluções em TRF para a polícia estadunidenses até que haja uma lei federal em vigor que garanta direitos humanos<sup>6</sup>.

A regulamentação apontada como necessária por estas empresas não é apenas aquela que autoriza o uso da tecnologia, já que mecanismos suficientes para assegurar direitos aos cidadãos devem ser criados - de forma oposta ao que foi previsto no PL em questão.

### c. Posicionamentos na Sociedade Civil

A página de internet **Ban Facial Recognition**<sup>7</sup> oferece dados compilados sobre a regulação em diversas cidades e estados dos EUA. Em junho de 2020, a demanda de banimento da tecnologia de reconhecimento facial ganhou uma dimensão nacional com o projeto de lei federal **Stop Biometric Surveillance by Law Enforcement Act**<sup>8</sup>. Ele é enfático na denúncia dos riscos que essa tecnologia oferece a direitos e liberdades civis e, caso aprovado, proibiria agências de segurança nacional de a utilizarem em câmeras corporais<sup>9</sup>. Ainda, a entidade *Amnesty International* criou o projeto **Ban the Scan** para divulgar os riscos da tecnologia e as maneiras de oposição ao uso de TRF pelas polícias americanas<sup>10</sup>.

<sup>5</sup> TILT. Após IBM, Amazon também proíbe seu reconhecimento facial para vigilância. 2020. Disponível em:

<https://www.bol.uol.com.br/noticias/2020/06/11/apos-ibm-amazon-tambem-proibe-seu-reconhecime-nto-facial-para-vigilancia.htm>. Acesso em 27 jan. 2020.

<sup>6</sup> ACB News. Microsoft joins Amazon, IBM in pausing face scans for police. 2020. Disponível em:

<https://abcnews.go.com/Business/wireStory/microsoft-joins-amazon-ibm-pausing-face-scans-police-71201516>. Acesso em 28 fev. 2021.

<sup>7</sup> BAN FACIAL RECOGNITION. Interactive Map. [S.l.], 2020. Disponível em:

<https://www.banfacialrecognition.com/map/>. Acesso em: 05 dez. 2020.

<sup>8</sup> CONGRESS. Text HR 7235. Disponível em:

<https://www.congress.gov/bill/116th-congress/house-bill/7235/text?r=50&s=1>. Acesso em: 3 mar. 2020.

<sup>9</sup> KIMERY, Anthony. Legislation would block police from using facial recognition with body cam footage. Biometric Update, [S.l.], 23 jun. 2020. Disponível em:

<https://www.biometricupdate.com/202006/legislation-would-block-police-from-using-facial-recogniti-on-with-body-cam-footage>. Acesso em: 05 dez. 2020.

<sup>10</sup> AMNESTY. Ban the Scan. 2020. Disponível em: <https://banthescan.amnesty.org/#global>. Acesso em: 28 jan. 2021.

Na Europa, entidades da sociedade civil<sup>11</sup> construíram um movimento chamado **Reclaim Your Face**<sup>12</sup>, que visa o banimento do uso de tecnologias de vigilância, principalmente as que utilizam dados biométricos como o uso de TRF, por serem dados sensíveis. A campanha se baseia na falta de transparência e informações sobre as ferramentas que estão sendo utilizadas e na necessidade e motivação para tanto.

Já na América Latina, a organização *Derechos Digitales* elaborou um projeto chamado **Reconocimiento Facial** para divulgar e conscientizar a população sobre os perigos da TRF. O objetivo principal da campanha é informar sobre o que está acontecendo na região em termos de uso de TRF, acompanhar o desenvolvimento dos esforços que estão sendo feitos neste campo e participar do debate a partir de uma perspectiva crítica baseada no respeito aos direitos humanos<sup>13</sup>.

Com isso, notam-se **movimentos da sociedade civil em diferentes regiões do mundo para banir o RF, especialmente quando usado pelo setor público, em vista da proteção dos direitos fundamentais de liberdade, privacidade e proteção de dados**. Diante do exposto, vários questionamentos são suscitados sobre se a TRF é adequada a espaços públicos e democráticos. Essas considerações são ainda mais sensíveis em vista dos limites técnicos dos sistemas atualmente disponíveis, considerando um viés discriminatório que afetaria sobremaneira grupos marginalizados.

### **3. Riscos do PL nº 865/19: direitos fundamentais, vigilância em massa, racismo, transfobia e direitos de crianças e adolescentes**

Com base em números de 2018, ano no qual **a rede metroferroviária paulista transportou 7,8 milhões de pessoas diariamente na região metropolitana de São**

---

<sup>11</sup> Várias organizações internacionais que defendem a liberdade de expressão e direitos digitais estão apoiando a campanha, a exemplo da Access Now, Article 19 e Panoptikon Foundation.

<sup>12</sup> RECLAIM YOUR FACE. The Movement. 2020. Disponível em: <https://reclaimyourface.eu/the-problem/>. Acesso em: 28 jan. 2021.

<sup>13</sup> RECONOCIMIENTO FACIAL. Sobre el proyecto. 2020. Disponível em: <https://reconocimientofacial.info/>. Acesso em: 28 jan. 2021.

**Paulo**<sup>14</sup>, não há como questionar o potencial lesivo da implementação de tecnologias de reconhecimento facial destinadas a um público tão amplo em utilização do transporte público. Há riscos que envolvem a coleta, o armazenamento, a integração de dados a outras bases e seu processamento enviesado - **questões que passaram ao largo do texto sintético aprovado, sem prescrição de garantias.**

É importante observar que as pessoas que não possuem outras formas de locomoção senão pelo transporte público estarão fadadas obrigatoriamente ao escaneamento constante de seus rostos. Ademais, **como conceber uma autorização legislativa tão genérica sem levar em conta notórios efeitos nocivos que a tecnologia impõe para a sociedade?**

Isso se agrava pelo fato de o PL utilizar expressões vagas como “preservar a segurança das pessoas” sem delimitação específica sobre como ou quem cumprirá esse objetivo, o que vai de encontro à noção de que qualquer redução a direitos deve ser feita com base em conceitos específicos e bem delimitados de modo a evitar ações autoritárias por parte do Estado.

Tecnologias de reconhecimento facial utilizam um método de identificação de pessoas por meio da distinção de seus rostos em vídeos, fotos ou imagens, em tempo real ou posteriormente à captura. Para permitir essa identificação, informações pessoais de tamanho e formato do rosto do indivíduo são capturadas, tratadas e convertidas em representações matemáticas denominadas *face template*, uma assinatura facial. Essa assinatura, resultante de tratamento de uma imagem capturada, é comparada com outras assinaturas disponíveis em bases de dados de assinaturas faciais e, assim, é feita a identificação<sup>15</sup>.

Uma peculiaridade nos chama atenção: **o dado pessoal tratado pela TRF é um dado biométrico, único e específico de cada pessoa**<sup>16</sup>. De acordo com a Lei Geral de

---

<sup>14</sup> SÃO PAULO. CPTM e Metrô: novas estações e 7,8 milhões de usuários por dia. Disponível em: [www.saopaulo.sp.gov.br/ultimas-noticias/cptm-e-metro-novas-estacoes-e-transporte-de-78-milhoes-de-pessoas-por-dia/](http://www.saopaulo.sp.gov.br/ultimas-noticias/cptm-e-metro-novas-estacoes-e-transporte-de-78-milhoes-de-pessoas-por-dia/). Acesso em: 26 fev. 2021.

<sup>15</sup>ELECTRONIC FRONTIER FOUNDATION (EFF). Face Recognition. 2017. Disponível em: <https://www.eff.org/pages/face-recognition>. Acesso em: 5. mai. 2020.

<sup>16</sup>THALES. Biometrics: authentication & identification (definition, trends, use cases, laws and latest news) - 2020 review. 2020. Disponível em:

Proteção de Dados (LGPD), esse tipo de dado, quando vinculado a uma pessoa natural, é um dado sensível<sup>17</sup>, que recebe tratamento distinto pela lei. Isso porque, caso eles “sejam conhecidos e submetidos a tratamento, podem se prestar a uma potencial utilização discriminatória ou lesiva e que apresentaria maiores riscos potenciais do que outros tipos de informação”<sup>18</sup>. Assim, e em decorrência desse entendimento, há riscos importantes que envolvem a TRF no contexto do PL nº 865/19:

### VIOLAÇÃO DE DIREITOS FUNDAMENTAIS

O Projeto de Lei nº 865/19 - ao autorizar o uso de TRF em contextos de segurança privada, deixando de delimitar a amplitude do compartilhamento de dados para fins de segurança pública - afronta a dignidade da pessoa humana, a privacidade, 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<sup>19</sup> em maio de 2020.

---

<https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/inspired/biometrics>. Acesso em: 5 mai. 2020.

<sup>17</sup>LGPD. Art. 5º Para os fins desta Lei, considera-se: (...) II - dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural.

<sup>18</sup> DONEDA, Danilo. Da privacidade à proteção de dados pessoais: elementos da formação da Lei geral de proteção de dados. 2a ed., São Paulo: Thomson Reuters Brasil, 2019. p. 143

<sup>19</sup>STF. Notícias STF. STF suspende compartilhamento de dados de usuários de telefônicas com IBGE. Disponível em: <http://www.stf.jus.br/portal/cms/verNoticiaDetalhe.asp?idConteudo=442902> Acesso em: 02 mar. 2021.

## VIGILÂNCIA EM MASSA

A vigilância em larga escala ocorre de forma irrestrita, sem definição prévia de um alvo específico e muitas vezes ininterruptamente. Se realizada em locais públicos, traz riscos à privacidade e à proteção de dados de um grande contingente populacional, que terá seus dados coletados e armazenados sem finalidades específicas e sem o consentimento nos termos da LGPD, que precisa ser expresso de forma livre, inequívoca e informada. A situação é ainda mais danosa se os dados coletados forem sensíveis, como são aqueles obtidos por tecnologias de reconhecimento facial<sup>20</sup>.

## RACISMO

Em razão de diferenças significativas quanto à acurácia de sistemas de reconhecimento facial na avaliação de rostos de pessoas não brancas, importa destacar que soluções em TRF não são neutras e refletem o racismo pré-existente na sociedade<sup>21</sup>. 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<sup>22</sup>.

## TRANSFOBIA

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

<sup>20</sup> REIS, Carolina. Nota Técnica. Lei 6.712/20. 10 Recomendações para o uso de reconhecimento facial para segurança pública no DF. LAPIN. 2021. Disponível em: <https://lapin.org.br/2021/02/22/nota-tecnica-lei-distrital-6712-2020-df/>. Acesso em: 01 mar. 2021.

<sup>21</sup> BUOLAMWINI, Joy; GEBRU; Timmit. Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification. Conference on Fairness, Accountability, and Transparency, Proceedings of Machine Learning Research 81, 1-15, 2018.

<sup>22</sup> BEUTIN, Lyndsey. Racialization as a Way of Seeing: The Limits of Counter-Surveillance and Police Reform. 2017. Surveillance & Society 15(1): 5-20.

sistemas de reconhecimento facial, os quais reiteradamente negam visibilização a identidades divergentes - conflitando com a auto-identificação de gênero<sup>23</sup>, acirrando violências e reiterando o cerceamento de direitos às pessoas transsexuais e não-binárias.

### VIOLAÇÃO DOS DIREITOS DE CRIANÇAS E ADOLESCENTES

A privacidade de crianças e adolescentes 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.<sup>24</sup> Pela impossibilidade de sistemas de TRF serem utilizados em espaços públicos como o dos transportes metroferroviários sem coletar dados de menores e incapazes, eles representam uma ameaça aos direitos de indivíduos dessa faixa etária.

## 4. Compartilhamento de dados pessoais

Apesar de o Projeto de Lei em análise não prever detalhes em termos de compartilhamento de dados pessoais sensíveis, como é o caso dos dados biométricos em questão, ele menciona **parcerias do Metrô e da CPTM com órgãos de segurança pública** para a eventual localização de pessoas foragidas a partir do sistema de reconhecimento facial.

A articulação entre a segurança da CPTM e do Metrô com as concessionárias do serviço de transporte ou mesmo entre elas e a Secretaria de Segurança Pública toma proporções complexas, já que atuam com objetivos que não necessariamente são complementares, já que envolvem interesses tanto privados quanto públicos. Trata-se,

<sup>23</sup> CODING RIGHTS. Reconhecimento Facial no Setor Público e Identidades Trans. Disponível em: <https://codingrights.org/docs/rec-facial-id-trans.pdf>. Acesso em: 28 fev. 2021.

<sup>24</sup> LGPD. Art. 14. O tratamento de dados pessoais de crianças e de adolescentes deverá ser realizado em seu melhor interesse, nos termos deste artigo e da legislação pertinente.

§1º O tratamento de dados pessoais de crianças deverá ser realizado com o consentimento específico e em destaque dado por pelo menos um dos pais ou pelo responsável legal.

então, de uma **multiplicidade de finalidades e repercussões legais** que devem ser avaliadas com cautela, pois dificultam o exercício da autodeterminação informativa<sup>25</sup>.

Há exemplos recentes que ilustram a potencialidade lesiva do uso de novas tecnologias quanto à vigilância em massa em contextos de compartilhamentos múltiplos. Em outubro de 2020, a Coalizão Direitos na Rede emitiu nota<sup>26</sup> sobre o sistema CórteX do Governo Federal<sup>27</sup>, que contaria com a capacidade de **cruzar as informações** com aquelas presentes em diversos bancos de dados, inclusive de outros entes da Administração Pública federal. A publicação menciona o vídeo de um capitão da Polícia Militar de São Paulo alegando ser possível obter os endereços de todos os funcionários de uma empresa a partir de seu CNPJ.

Assim, **o que impediria que uma integração similar de sistemas que enriquecesse bases com dados biométricos capturados nas estações de trem e metrô não fosse criada?** Essa separação parece ainda nebulosa no bojo do Projeto de Lei aqui analisado por uma característica que perpassa todo seu texto: a **ausência de salvaguardas adequadas** para garantir a proteção de dados e da privacidade.

## 5. Proteção de dados pessoais e direitos dos titulares

A LGPD tem por objetivo garantir a autonomia do indivíduo sobre suas informações pessoais. Uma das principais exigências da lei é a observância dos princípios de proteção de dados no tratamento de informação e a garantia do exercício dos direitos dos titulares de dados pessoais. **Como lei geral, os seus princípios e direitos se**

---

<sup>25</sup> O reconhecimento de um direito à autodeterminação informativa deu-se pela primeira vez pela Corte Constitucional alemã, em 1983; trata-se da concepção de que não mais existiriam dados insignificantes nas circunstâncias modernas do processamento automatizado de dados e que é necessário garantir o controle do indivíduo quanto ao fornecimento e utilização dos seus dados pessoais. MENDES, Laura Schertel Ferreira. Autodeterminação informativa: a história de um conceito. Pensar, Fortaleza, v. 25, n. 4, p.1-18, out./dez. 2020. Disponível em: <https://periodicos.unifor.br/rpen/article/view/10828/pdf>. Acesso em: 2 mar. 2021.

<sup>26</sup> CDR. Sistema CórteX, do governo federal, ameaça direitos dos cidadãos. 2020. Disponível em: <https://direitosnarede.org.br/2020/10/01/sistema-cortex-do-governo-federal-ameaca-direitos-dos-cidadaos/>. Acesso em: 1 mar 2021.

<sup>27</sup> REBELLO, Auri. Conheça o CórteX. 2020. Disponível em: <https://theintercept.com/2020/09/21/governo-vigilancia-cortex/>. Acesso em: 1 mar. 2021.

**aplicam amplamente ao contexto de tratamento de dados, incluindo casos voltados à promoção de segurança**, seja ela pública ou privada, conforme art. 4º, III, da Lei.

Inicialmente, falta uma análise adequada por parte do poder público da compatibilidade do uso de reconhecimento facial com o objetivo pretendido. De acordo com o **princípio da necessidade**, previsto na LGPD em seu art. 6º, III, o tratamento de dados deve ser reduzido ao mínimo necessário para a realização das finalidades pretendidas, devendo esses dados serem proporcionais e não excessivos em relação às finalidades do tratamento de dados.

Considerando que as estações e vagões de metrô e trem são espaços frequentados diariamente por milhares de pessoas, muitas das quais não possuem outras opções de transporte, levanta-se a questão de se expô-las a tamanho grau de vigilância pelo Estado é realmente necessário.

Dados biométricos, como os coletados pela TRF, são de difícil alteração. Logo, o alto risco de falhas de segurança que podem expor dados tão valiosos, bem como a falta de um relatório de impacto à proteção de dados que de fato reconheça se a razão entre a identificação de procurados e a quantidade massiva de dados coletados de indivíduos é efetiva o suficiente, levanta a dúvida de se tal tratamento de dados é de fato necessária e proporcional. O fato de não haver uma resposta para isso pelo Legislativo estadual, ou a resposta ser meramente retórica, como a apresentada na exposição de motivos do PL, demonstra uma falta de justificativa que permita a conclusão de que o tratamento realmente é compatível com os princípios da LGPD.

Para além dos princípios da LGPD, os principais direitos de que dispõe são elencados em seu Capítulo III, incluindo a confirmação de ocorrência de tratamento e uso compartilhado, bem como a possibilidade de acesso, correção e eliminação dos dados pessoais coletados. **O Projeto de Lei, entretanto, não traz qualquer menção a esses direitos ou à forma de seu exercício.** Nesse sentido, para que seja aprovado sem atentar à lei federal, deve apresentar indicações suficientes para que permita aos indivíduos acessarem seus direitos.

Também é necessário determinar quais as **bases legais** aplicáveis para o tratamento de dados sensíveis nesse contexto, dentre as previstas na LGPD em seu artigo 11, se aplica ao uso de TRF pretendido pelo sistema metroferroviário. Tal avaliação é primordial para se realizar um juízo a respeito da legalidade do tratamento de dados pretendido pelo PL, o que inclui uma análise a respeito da estrita necessidade e proporcionalidade do uso de uma tecnologia tão intrusiva<sup>28</sup>.

A mera existência de lei estadual que determine o tratamento de dados sensíveis, sem que haja adequação entre a finalidade e as bases legais cabíveis presentes na LGPD, **infringe desproporcionalmente o direito fundamental à proteção de dados pessoais**. Não bastasse, o PL não traz nenhuma salvaguarda para que titulares exerçam seus direitos face ao cenário de coleta massiva de dados pessoais sensíveis que o Projeto propõe. Isso se agrava pelo fato de que os indivíduos a elas expostos não necessariamente têm outra escolha se não o uso de transporte público, que automaticamente obrigará a coleta de seus dados e imporá evidente impacto ao exercício de seu direito fundamental à autodeterminação informativa.

## 6. Uso Ineficiente de Recursos Públicos

De acordo com o art. 1º, o projeto de lei tem o intuito de utilizar a tecnologia para “preservar a segurança das pessoas, evitando riscos à vida ou a integridade das mesmas, por ação de quadrilhas ou criminosos individuais”. Contudo, como observado acima, **a TRF pode ser incerta, imprecisa e propensa a abusos, fazendo com que recursos públicos sejam utilizados de maneira ineficiente**.

Esse é o caso particularmente dos falsos positivos. De acordo com estudo do Panóptico, por exemplo, durante o teste da tecnologia realizado na Copa América no Estádio Maracanã, **63% das pessoas foram identificadas incorretamente**.<sup>29</sup> Outros casos também de identificação errônea já foram reportados em testes em outros

---

<sup>28</sup> Council of Europe. **Guidelines on Face Recognition**. Directorate General of Human Rights and Rule of Law, 28 jan 2021.

<sup>29</sup> Panóptico. Disponível em: <https://opanoptico.com.br>.

lugares. Em Copacabana, uma senhora foi confundida com uma pessoa acusada de homicídio.<sup>30</sup> Na Bahia, um jovem foi confundido com acusado de assalto.<sup>31</sup> Nesses casos, **recursos públicos podem ser despendidos para atuar frente a equívocos da tecnologia, desviando-os de seu devido fim.**

Ante a impossibilidade de se atingir o fim que pretende, o projeto de lei ofende ao postulado da proporcionalidade. O primeiro passo para verificar a obediência ao princípio é a adequação de uma medida, isto é, as possibilidades dela 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.

Da mesma forma, existem meios menos gravosos e onerosos de se atingir um resultado ainda mais eficaz, a título exemplificativo, a mera instalação de câmeras sem reconhecimento facial. Evitar-se-ia os falsos positivos, a violação à liberdades e direitos fundamentais, tal como o risco de discriminação.

Dessa forma, o projeto de lei almeja fim legítimo e louvável, todavia por meio potencialmente **inadequado** e **ineficaz**. Por sua vez, a utilização desnecessária de recursos onera o erário público além de prejudicar a fiscalização, portanto atenta contra o interesse público.

---

<sup>30</sup> FANTTI, Bruna. Reconhecimento facial falha e mulher é detida por engano. O Dia, 10 de julho de 2019. Disponível em: <https://odia.ig.com.br/rio-de-janeiro/2019/07/5662023-reconhecimento-facial-falha-e-mulher-e-detida-por-engano.html>.

<sup>31</sup> PALMA, Amanda e PACHEO, Clarissa. 'O policial já foi com a arma na cabeça dele', diz mãe de rapaz confundido por reconhecimento facial'. Correio 24hrs. 5 de janeiro de 2020. Disponível em: <https://www.correio24horas.com.br/noticia/nid/o-policial-ja-foi-com-a-arma-na-cabeca-dele-diz-mae-de-rapaz-confundido-por-reconhecimento-facial/>.

## 7. Conclusão

Face a problemas sociais tão complexos como a violência urbana, muitas vezes a tecnologia é tida como uma bala de prata para sua superação. No entanto, nem sempre a solução tecnológica escolhida é a mais adequada para atingir os fins buscados.

Os exemplos citados demonstram a falta de estudos conclusivos que comprovem a eficiência da TRF para segurança, ao passo que há uma série de apontamentos em termos de potenciais **violações a liberdades e direitos fundamentais**, os quais não podem ser ignorados. A incompatibilidade do Projeto de Lei em relação aos princípios e direitos da LGPD é mais um agravante a isso, já que representa a ausência de análises mais completas que demonstram a proporcionalidade do uso dessa tecnologia na forma como se pretende.

Tendo esse cenário em vista, sugerimos ao Estado de São Paulo que adote a **precaução**<sup>32</sup> como princípio, no sentido de evitar utilizar uma tecnologia que é fruto de tamanhos questionamentos éticos e legais de forma a zelar pelos direitos dos cidadãos. Há riscos graves tanto em termos de violações a direitos fundamentais quanto de baixo adensamento social da matéria, de gastos públicos que podem não ter retorno e de provável judicialização em escala do tema.

O Projeto de Lei nº 865/2019 foi aprovado **sem debate público amplo sobre a matéria** e está atrelado a potenciais ilegalidades e violações de direitos fundamentais. Portanto, defendemos que **tal projeto de lei seja vetado** da forma como está redigido. Caso o tema retorne à pauta da Assembleia Legislativa, indicamos que seja objeto de discussão abrangente, de modo a permitir uma avaliação extensiva e detalhada para julgar a real necessidade e proporcionalidade do uso da tecnologia para a finalidade pretendida.

---

<sup>32</sup> BIONI, Bruno Ricardo; LUCIANO, Maria. O Princípio da Precaução na Regulação de Inteligência Artificial: seriam as Leis de Proteção de Dados o seu portal de entrada? 2020. Disponível em: [https://brunobioni.com.br/wp-content/uploads/2019/09/Bioni-Luciano\\_0-PRINCI%CC%81PIO-DA-PRECAUC%CC%A7A%CC%830-PARA-REGULAC%CC%A7A%CC%830-DE-INTELIGE%CC%82NCIA-ARTIFICIAL-1.pdf](https://brunobioni.com.br/wp-content/uploads/2019/09/Bioni-Luciano_0-PRINCI%CC%81PIO-DA-PRECAUC%CC%A7A%CC%830-PARA-REGULAC%CC%A7A%CC%830-DE-INTELIGE%CC%82NCIA-ARTIFICIAL-1.pdf). Acesso em: 01 mar. 2021.

Isto posto, as **organizações abaixo listadas** se unem para instar o veto total ao PL 865/2019 SP, por ser inconstitucional e contrário ao interesse público para a proteção de direitos fundamentais e, na forma como está proposto, ser medida desproporcional para atingir ao fim almejado.

### **Lista de organizações:**

Access Now

Centro de Estudos da Mídia Alternativa Barão de Itararé

Instituto Beta: Internet & Democracia (IBIDEM)

Instituto de Referência em Internet e Sociedade (IRIS BH)

Instituto de Tecnologia e Sociedade do Rio (ITS-Rio)

Laboratório de Políticas Públicas e Internet (LAPIN)

