INSTITUTO IGARAPÉ
a think and do tank

DataPrivacyBR
RESEARCH


# REGULAÇÃO DO RECONHECIMENTO FACIAL NO SETOR PÚBLICO:

## avaliação de experiências internacionais

# SUMÁRIO



# AUTORES

Pedro Augusto P. Francisco - Pesquisador sênior no Instituto Igarapé
Louise Marie Hurel - Pesquisadora plena no Instituto Igarapé
Mariana Marques Rielli - líder de projetos no Data Privacy Brasil Research

Arte capa: Raphael Durão

# REGULAÇÃO DO RECONHECIMENTO FACIAL NO SETOR PÚBLICO:
## avaliação de experiências internacionais

# SUMÁRIO EXECUTIVO


- A expansão do emprego de sistemas de reconhecimento facial pelo setor público vem despertando, ao mesmo tempo, expectativas e preocupações a respeito dos impactos negativos dessas tecnologias. Mesmo com o crescimento de iniciativas de uso dessa ferramenta, ainda falta entendimento sobre como estão sendo empregadas dentro de um contexto de realidades nacionais, incluindo o Brasil, e clareza sobre como pensar padrões e regulações para tal.

- Diante desse cenário, o Instituto Igarapé e o Data Privacy Brasil Research elaboraram o presente documento, com o objetivo de apresentar diferentes abordagens e estratégias de regulação dos sistemas de reconhecimento facial, proporcionando um panorama para auxiliar legisladores e gestores públicos na reflexão, no debate e na criação de normas para uma utilização responsável dessa tecnologia pelo setor público.

- No âmbito internacional, selecionamos três países que nos apresentam distintas abordagens de autorização, que se desdobram em estratégias de regulação, do uso de sistemas de reconhecimento facial pelo setor público. Inglaterra, Estados Unidos e França trazem diferentes práticas, cada uma delas com lições a serem aprendidas por legisladores e gestores públicos no Brasil. Cada um dos três casos foi analisado a partir dos princípios da finalidade, necessidade, transparência, segurança da informação e não-discriminação.

- No contexto nacional, fizemos um levantamento dos projetos de lei existentes nos âmbitos federal, estadual e municipal. Os projetos foram analisados de maneira aprofundada, para em seguida serem comparados dentro do enquadramento dos mesmos princípios utilizados como parâmetros no âmbito internacional.

- Na sequência, comparamos os três cenários internacionais com o atual cenário brasileiro: os alinhamentos, divergências, pontos fortes e fracos de cada uma das abordagens.

- As regulações sobre o uso de sistemas de reconhecimento facial ainda se encontram em estágio experimental. Para serem eficientes, as futuras abordagens precisam considerar as rápidas mudanças nas tecnologias de monitoramento de dados biométricos, buscando antecipar novas aplicações e funcionalidades.

- Qualquer regulação também deve ser precedida de um amplo debate público, travado de modo acessível e transparente. Somente assim será possível criar instrumentos regulatórios que contemplem a perspectiva de especialistas e de todos os grupos potencialmente afetados pelo emprego da tecnologia. Isso garante a proteção de dados e a elaboração de estratégias para mensurar impactos.

- Finalmente, é importante considerar que nenhuma nova regulação sobre os sistemas de reconhecimento facial são criadas em um vácuo normativo. Legisladores e gestores públicos precisam harmonizar qualquer experiência regulatória dessas tecnologias com os marcos legais que dispõem sobre a garantia da privacidade e da proteção de dados.

# 1. INTRODUÇÃO E ESCOPO

A expansão das atividades de videomonitoramento urbano tem sido uma das principais respostas ao problema da violência na América Latina. Com frequência, essas tecnologias são consideradas e utilizadas como aliadas do setor público e ganham protagonismo na segurança pública. Nesse cenário, podem servir como mecanismo de prevenção ao crime quando empregadas em conjunto com processos e práticas eficientes de policiamento, proporcionando apoio em um ambiente de recursos limitados.

Dentro do rol de tecnologias de videomonitoramento, destaca-se a expansão dos sistemas de reconhecimento facial, que tem recebido grande atenção de autoridades públicas no Brasil. Até maio de 2019, foram pelo menos 48 casos publicamente reportados de implementação dessa ferramenta por autoridades públicas. Desses casos, 13 tinham a garantia da segurança pública como principal objetivo[1].

Na América Latina, outras cidades seguem a tendência e vêm testando diferentes sistemas de reconhecimento facial, como Buenos Aires, Córdoba, Mendoza, Lima e Coahuila[2]. Trata-se de um caminho que desperta preocupações em toda a região, devido ao potencial de vigilância em massa, às possíveis violações às liberdades individuais, à proteção de dados e à falta de experiências e estudos sobre seus impactos negativos. Além disso, em países como o Brasil e outros da América Latina, essas mesmas preocupações se somam à falta de transparência sobre a aquisição e implementação dos sistemas de reconhecimento facial, bem como sobre seus protocolos de uso e métodos de coleta dos dados[3]. Em contextos onde as desigualdades de classe, raça e gênero já são marcantes, o mau uso de tecnologias de vigilância, cujo funcionamento depende da aplicação de inteligência artificial, pode ser ainda mais prejudicial.

Todo esse cenário se tornou ainda mais grave no início de 2020, quando o mundo se viu afetado por uma pandemia de proporções globais. Conforme a COVID-19 se espalha por uma grande parcela da população, colocando os sistemas de saúde em risco de colapso e já apontando para uma crise econômica extremamente grave, governos do mundo inteiro vêm buscando soluções tecnológicas para ajudar no combate à pandemia. Entre as soluções apresentadas, está a utilização dos sistemas de reconhecimento facial, como no caso da Rússia[4] e China[5], que vêm empregando a tecnologia para garantir que pessoas infectadas ou em quarentena não saiam do regime de isolamento.

Diante desse novo cenário de adoção progressiva e iminente de uma ferramenta que ainda apresenta tantos riscos, surge a necessidade de se pensar uma regulação eficiente que permita, ao mesmo tempo, o uso responsável e a garantia da preservação

1 Ver infográfico em https://igarape.org.br/infografico-reconhecimento-facial-no-brasil/

2 MUGGAH, R. & FRANCISCO, P. Fev. (2020). Brazil's Risky Bet on Tech to Fight Crime. *Americas Quarterly*. Disponível em: https://www.americasquarterly.org/article/brazils-risky-bet-on-tech-to-fight-crime/

3 RODRIGUEZ, K. Dez. (2019). Activists Worldwide Face Off Against Face Recognition: 2019 Year in Review. *EFF*. Disponível em: https://www.eff.org/deeplinks/2019/12/activists-worldwide-face-against-face-recognition-2019-year-review

4 REUTERS. Fev. (2020). *Moscow deploys facial recognition technology for coronavirus quarantine.* Disponível em: https://br.reuters.com/article/idUSKBN20F1RZ

5 FINANCIAL TIMES. Abr. (2020) *China, coronavirus and surveillance: the messy reality of personal* data. Disponível em: https://www.ft.com/content/760142e6-740e-11ea-95fe-fcd274e920ca

de direitos. Os benefícios públicos precisam ser amplamente debatidos, com a garantia de salvaguardas para a proteção de dados e estratégias que sejam capazes de mensurar os impactos da tecnologia. Qualquer regulação que seja desenvolvida especificamente para o uso e implementação de reconhecimento facial pelo setor público deve ser regida por princípios claros e transparentes, que permitam a responsabilização das instituições envolvidas.

Foi pensando nessa necessidade que o Instituto Igarapé e o Data Privacy Brasil Research desenvolveram o presente trabalho. Aqui, apresentamos uma análise comparativa das principais iniciativas e tendências regulatórias que têm os sistemas de reconhecimento facial como objeto. Com este documento, fornecemos aos legisladores e gestores públicos um instrumento que pode ajudá-los na reflexão, no debate e na criação de normas para uma utilização responsável dessa tecnologia pelo setor público, tendo como base o que já vem sendo feito no Brasil e em outros países do mundo.

# 2. METODOLOGIA

Nossa análise foi dividida em diferentes etapas. No âmbito internacional, selecionamos três países que nos apresentam distintas abordagens de autorização do uso de sistemas de reconhecimento facial pelo setor público, que se desdobram em estratégias de regulação. Inglaterra, Estados Unidos e França trazem diferentes abordagens, cada uma delas com lições a serem aprendidas por legisladores e gestores públicos no Brasil.

O caso inglês mostra um cenário onde o uso dos sistemas de reconhecimento facial é autorizado, dando origem a uma estratégia de regulação cujo objetivo é enquadrar os a tecnologia dentro do ordenamento jurídico pré-existente, a partir de publicações de documentos recomendatórios, que orientam seu uso responsável. Na França, a abordagem também autoriza o setor público a adotar as ferramentas de reconhecimento facial, porém apenas mediante a aprovação de órgãos competentes. Trata-se de uma etapa intermediária, na qual o governo francês reconhece a necessidade da avaliação dos impactos da tecnologia para posteriormente desenvolver uma regulação específica. Por fim, o caso dos EUA nos apresenta uma abordagem mais direta de não-autorização, com regulações que buscam banir o uso dos sistemas de reconhecimento facial, até que se produzam dados suficientes para compreender seus impactos.

Cada um dos três casos foi analisado a partir dos princípios da finalidade, necessidade, transparência, segurança da informação e não-discriminação. Esses princípios foram escolhidos por serem centrais na Lei Geral de Proteção de Dados brasileira (Lei 13.709/2018), na *General Data Protection Law*, da União Europeia, e nos ordenamentos jurídicos do Reino Unido e dos EUA. A análise foi feita a partir da seleção dos principais instrumentos legais e documentos oficiais dos três países que tratam diretamente da regulação dos aparatos de videomonitoramento ou biometria. Assim, foi possível avaliá-los à luz dos princípios e traçar um panorama de como são contemplados nesses cenários.

No âmbito nacional, fizemos um levantamento dos projetos de lei existentes nos âmbitos federal, estadual e municipal. Os projetos foram analisados de maneira aprofundada, para em seguida serem comparados dentro do enquadramento dos mesmos princípios utilizados como parâmetros no âmbito internacional.

## *Princípios e critérios de análise:*

A análise dos documentos e instrumentos legais que realizamos teve como base o modo como estes lidavam com cinco aspectos básicos da proteção de dados pessoais, sintetizados em princípios já previstos em lei. A escolha por avaliar as iniciativas de regulação dos sistemas de reconhecimento facial a partir desses cinco princípios se dá por uma razão muito simples: o funcionamento desses sistemas depende do tratamento de dados pessoais. Para que qualquer sistema de reconhecimento facial funcione, é preciso que uma ou mais câmeras capturem a imagem de um rosto. Essa imagem será convertida em dados que correspondem a diversas características particulares da face de uma pessoa que, posteriormente, serão analisadas para o tratamento que se pretende. Tratam-se de dados resultantes de um tratamento específico de elementos físicos e fisiológicos - e eventualmente até mesmo comportamentais - singulares de uma pessoa, que permitem sua identificação. Isso significa que o reconhecimento facial funciona com base no tratamento de dados biométricos.

Assim, qualquer emprego de sistemas de reconhecimento facial no Brasil deverá respeitar os princípios que utilizamos como critério de análise, tendo em vista sua previsão na Lei Geral de Proteção de Dados.

Abaixo, elencamos os cinco princípios selecionados e os critérios utilizados para analisar como foram abordados nos documentos e instrumentos estudados.

*Finalidade*: a finalidade diz respeito aos propósitos que orientam o tratamento de dados pessoais. Estes devem ser sempre legítimos, específicos e explícitos, bem como não deve haver tratamento posterior que seja incompatível com essas finalidades. Em nossa análise, o princípio da finalidade foi observado a partir de dois critérios. Primeiramente, buscamos entender como os documentos e legislações justificavam a regulação dos sistemas de reconhecimento facial, seja para utilizá-los ou proibi-los. Em segundo lugar, observamos se havia alguma menção expressa dessas finalidades ao longo do texto.

*Necessidade*: o princípio da necessidade relaciona-se diretamente à finalidade, apesar de não se confundir com a mesma. Aqui, procura-se garantir que o tratamento de dados pessoais seja restrito somente ao uso que se pretende, ou seja, ele deve ser limitado da melhor forma possível à necessidade do agente que coleta e trata os dados. Novamente, nossa análise do princípio da necessidade fez uso de dois critérios. O primeiro foi observar quais eram os limites impostos aos sistemas de reconhecimento facial. O segundo buscou compreender quais eram os protocolos de uso desses mesmos sistemas.

*Transparência*: o princípio da transparência busca garantir que todos os titulares dos dados pessoais que serão tratados sejam informados a respeito desse tratamento. Essas informações precisam ser claras e de fácil acesso. Entende-se que, em certas situações, não será possível fornecer muitos detalhes, seja por razões de segredo industrial sobre a tecnologia empregada, ou em consequência da finalidade do tratamento, como por exemplo, nos casos em que os dados são usados para fins de segurança pública ou segurança nacional. Ainda assim, os titulares sempre terão o direito de acessar informações em linguagem acessível e simples sobre a realização do tratamento. Nossa análise buscou examinar a transparência a partir de um critério: se os documentos e as legislações apresentavam alguma política de transparência e comunicação aos cidadãos sobre o uso dos sistemas de reconhecimento facial.

*Segurança da informação*: o princípio da segurança tem como objetivo garantir que o tratamento de dados pessoais será feito de modo a atender critérios razoáveis de segurança e confidencialidade, evitando perda, destruição, alterações e vazamentos dos dados, bem como promovendo a utilização de ferramentas e políticas de proteção dos mesmos. Em nossa análise, buscamos avaliar o princípio da segurança em dois critérios. Primeiramente, observamos se os documentos e legislações promovem a utilização de medidas técnicas para a proteção dos dados coletados pelos sistemas de reconhecimento facial. Em seguida, averiguamos se havia alguma disposição expressa sobre o período de retenção dos dados.

*Não-discriminação*: este princípio determina que nenhum tratamento de dados pessoais pode ser realizado com fins discriminatórios, ou seja, não deve haver nenhuma forma de impacto ilegítimo nos titulares em consequência de características de gênero e orientação sexual, origem racial e social, posicionamento político, religião ou estado de saúde. Mais uma vez, nossa análise dos documentos e legislações utilizou dois critérios para avaliar a observância do princípio da não-discriminação. Em primeiro lugar, analisamos se havia algum cuidado ou menção de mecanismos que evitassem qualquer viés social no uso de sistemas de reconhecimento facial. Em segundo lugar, buscamos identificar se havia a previsão da realização de avaliações de impacto social desses mesmos sistemas.

# 3. EXPERIÊNCIAS INTERNACIONAIS

O desenvolvimento dos sistemas de reconhecimento facial não é um fenômeno recente. Desde os anos 1960, técnicas de computação vêm sendo criadas para detectar padrões, reconhecer e identificar um rosto humano[6]. Porém, a recente expansão das capacidades de processamentos, coleta e armazenamento de dados, a disseminação de sensores e dispositivos, e o aprimoramento de algoritmos de inteligência artificial permitiram que esses sistemas fossem explorados comercialmente e empregados por diversos órgãos públicos ao redor do mundo[7]. Esse rápido crescimento colocou autoridades públicas, empresas e sociedade civil em uma encruzilhada: como regular o uso dessa tecnologia, de modo a aproveitar os seus potenciais e ao mesmo tempo preservar o exercício dos direitos e liberdades civis?

Atualmente, não há uma resposta definitiva para essa pergunta. Mesmo após 60 anos desde o surgimento dos primeiros sistemas de reconhecimento facial, seu emprego massivo é relativamente recente. Trata-se, afinal, de uma tecnologia experimental. Não obstante, alguns países vêm tentando acompanhar o desenvolvimento e a utilização desses sistemas, apresentando diferentes abordagens de autorização do uso, acompanhadas por estratégias regulatórias. Ressaltamos que nenhuma delas pode ser considerada como bem-sucedida, pois ainda é preciso compreender seus impactos.

Para a análise apresentada aqui, selecionamos três dessas abordagens. Em momento algum almejamos exaurir todas as possibilidades. Como ressaltamos no início, nosso objetivo é

6 DE LEEUW, K. & BERGSTRA, J. Jan. (2007). *The History of Information Security: A Comprehensive Handbook*. Amsterdam: Elsevier.

7 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

mostrar cenários interessantes que já vêm se desenhando no mundo, para que legisladores e gestores públicos tenham parâmetros de comparação, caso queiram construir um caminho para a regulação dos sistemas de reconhecimento facial no Brasil.

# *REINO UNIDO*

Quando se discute o emprego de qualquer sistema de monitoramento por parte de órgãos públicos, o Reino Unido é provavelmente o primeiro cenário a ser observado. Já em 1953, o governo britânico instalou seu primeiro circuito-fechado de TV, instalando câmeras para garantir a segurança da cerimônia de coroação da Rainha Elizabeth II[8]. Desde então, a infraestrutura de câmeras de vigilância se expandiu no país, alcançando o impressionante número de 6 milhões[9]. Os sistemas de reconhecimento facial, por sua vez, são usados por polícias no Reino Unido desde 1998[10].

O longo período de experiência com sistemas de videomonitoramento e a constante pressão e preocupação da sociedade civil com as possíveis violações aos direitos civis que eles ensejam, principalmente com relação à privacidade e às liberdades de expressão e associação em espaços públicos, fizeram com que o Reino Unido desenvolvesse uma robusta legislação sobre o tema ao longo dos anos. Além disso, foi criado um verdadeiro ecossistema de instituições governamentais que têm por responsabilidade monitorar diferentes aspectos do aparato de monitoramento estatal.

Esse cenário permitiu ao Reino Unido autorizar o uso e adotar, até o momento, uma estratégia particular para regular o emprego dos sistemas de reconhecimento facial. Não há nenhum instrumento legal específico voltado para a regulação desse tipo de tecnologia, mas sim uma série de documentos estratégicos e recomendatórios que procuram enquadrá-la dentro do arcabouço jurídico pré-existente, além de apontar diretrizes para um emprego responsável por parte dos órgãos da administração pública.

Na tabela abaixo, analisamos como o cenário britânico lida com os sistemas de reconhecimento facial, e como se enquadra nos cinco princípios que escolhemos para avaliá-lo. Os documentos analisados foram:

- Biometrics Strategy: Better public services Maintaining public trust;
- Surveillance Camera Code of Practice;
- ICO Code of Practice for Surveillance Cameras;
- Metropolitan Police Legal Mandate for deploying Live Facial Recognition.

8 BBC. Nov. (2006). *How we are being watched*. Disponível em: http://news.bbc.co.uk/2/hi/uk_news/6110866.stm

9 CARLO, S. Mai. (2019). Britain Has More Surveillance Cameras Per Person Than Any Country Except China. That's a Massive Risk to Our Free Society. *Time*. Disponível em: https://time.com/5590343/uk-facial-recognition-cameras-china/

10 DEVLIN, H. Oct. (2019). "We are hurtling towards a surveillance state": the rise of facial recognition technology. *The Guardian*. Disponível em: https://www.theguardian.com/technology/2019/oct/05/facial-recognition-technology-hurtling-towards-surveillance-state

## **Tabela 1.** Reino Unido

| | | |
|---|---|---|
| Finalidade | 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. |
| | Há alguma menção expressa sobre as finalidades autorizadas ou proibidas? | Controle de imigração; investigação, detecção e prevenção de atividades criminosas e terroristas; segurança nacional e segurança pública; bem-estar econômico do país; prevenção de desordem; proteção da saúde ou da moral; proteção de direitos e liberdades. |
| Necessidade | 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.<br><br>Para os casos de vigilância em espaços públicos, não se pode presumir o consentimento da 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 justificativa para o emprego em local público precisam ser revistas anualmente. |
| | Quais são os protocolos de uso desses sistemas? | Há a previsão, por parte do Home Office, de criar um conselho supervisor e consultivo para coordenar considerações a respeito do uso de sistemas de reconhecimento facial por parte das forças de segurança, incluindo recomendações sobre protocolos. O conselho será composto por representantes do Home Office, do Surveillance Camera Commissioner's Office, do Biometrics Commissioner's Office, do Information Commissioner's Office, do Forensic Science Regulator e do Biometrics and Forensics Ethics Group.<br><br>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.<br><br>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. |
| Transparência | 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.<br><br>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.<br><br>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. |

**Tabela 1.** Reino Unido (continuação)

| | | |
|---|---|---|
| Segurança | 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. |
| | Existe alguma disposição expressa sobre o período de retenção desses mesmos dados? | A regulação determina que, após uma prisão, a polícia pode registrar uma foto do indivíduo e mantê-la sob custódia e armazená-la em sistemas locais, bem como na Police National Database. Contudo, indivíduos absolvidos ou cujas acusações foram retiradas podem requisitar a remoção de suas imagens do sistema.<br><br>Em todos os outros casos, imagens e informações coletadas por câmeras não podem ser armazenadas por mais tempo do que seja necessário para sua finalidade. Contudo, não há nenhuma determinação de período específico, ficando este a critério da instituição responsável por seu armazenamento. De qualquer forma, o período escolhido precisa ser informado e justificado ao público.<br><br>Especificamente sobre reconhecimento facial, algumas forças policiais eliminam dados coletados pelas câmeras automaticamente, quando não há nenhum tipo de alerta do sistema. Na ocasião em que ocorre um alerta, os dados são deletados o mais rápido possível após a tomada de decisão, dentro de um limite máximo de 31 dias. |
| Não-discriminação | Existe algum cuidado ou menção sobre o risco de viés social no uso de sistemas de reconhecimento facial? | No Reino Unido, qualquer uso de dados biométricos deve ter seus aspectos éticos avaliados pelo Biometrics and Forensics Ethics Group, mesmo que atenda aos critérios legais. |
| | Existe a previsão da realização de avaliações de impacto social desses mesmos sistemas? | O Reino Unido tem como estratégia futura a realização de avaliações de impacto antes do emprego de qualquer novo sistema que utilize dados biométricos, ou mesmo para novas aplicações de sistemas já existentes.<br><br>Além disso, existem recomendações para a realização de avaliações de impacto à privacidade sempre que houver emprego de câmeras de vigilância, com revisões regulares. |

# *ESTADOS UNIDOS*

O uso de sistemas de reconhecimento facial nos Estados Unidos é vasto, de modo que não é possível afirmar que o país segue dentro de uma abordagem única. No entanto, o país vem se destacando através de vários legisladores municipais, bem como de alguns projetos de lei estaduais, que adotaram o caminho da não autorização dessa tecnologia.

Essa abordagem, que pode ser interpretada como radical, tem como princípio que os sistemas de reconhecimento facial não podem ser empregados sem um debate público que exponha as custos e os riscos dessa tecnologia. Os proponentes do banimento nos EUA defendem que a capacidade de precisão dos sistemas e os potenciais benefícios setoriais não podem se sobrepor ao debate sobre direitos e proporcionalidades do uso. Os argumentos partem do princípio de que a coleta de dados biométricos dos rostos de indivíduos possui um alto grau de sensibilidade, constituindo-se assim como um monitoramento intrusivo, podendo ser realizado sem que o titular dos dados tenha conhecimento da coleta e do tratamento[11].

Abaixo, a tabela mostra como o conjunto de iniciativas que baniram ou procuram banir os sistemas de reconhecimento facial em diversas cidades e estados dos EUA se enquadram nos princípios que serviram como base de nossas análise. As legislações e projetos de lei examinados foram:

- California AB-1215: “Law enforcement: facial recognition and other biometric surveillance”;
- San Francisco Ordinance 190110 - “Stop Secret Surveillance”;
- City of Alameda Resolution nº 15625 / 2019;
- Oakland City Council Ordinance nº 13563 / 2019;
- Northampton, MA Ordinance nº 19.176;
- Brookline Warrant Article 25 / Nov. 19, 2019;
- Somerville Ordinance nº 2016-16;
- Massachusetts Senate Bill 1385/House Bill 1538;
- New Hampshire House Bill 1642-FN;
- State of Washington House Bill 2856;
- Michigan Senate Bill 342;
- Michigan House Bill 4810;

11 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

## **Tabela 2.** Estados Unidos

| | | |
|---|---|---|
| Finalidade | Como os documentos e legislações analisados justificam a regulação dos sistemas de reconhecimento facial? | A regulação que propõe o banimento ou moratória dos sistemas de reconhecimento facial é categórica em suas justificativas, baseando-se principalmente na proteção dos direitos individuais e liberdades civis, estebelecidas em preceitos da Constituição dos EUA ou nas Constituições dos Estados. |
| | Há alguma menção expressa sobre as finalidades autorizadas ou proibidas? | Em geral, a finalidade da proibição ao uso de sistemas de reconhecimento facial baseia-se na prevenção dos danos que estes podem causar à privacidade, à liberdade de expressão e de associação em espaços públicos. Também apontam que esses sistemas são uma ameaça ao devido processo legal, pois invertem o princípio da presunção de inocência ao tratar todos os cidadãos como suspeitos potenciais |
| Necessidade | Quais são os limites impostos aos sistemas de reconhecimento facial? | As regulações proibem a aquisição, posse, acesso ou uso de sistemas de reconhecimento facial, ou de qualquer dado obtido por meio desses sistemas, por parte de órgãos ou funcionários públicos das cidades e estados onde estejam em vigor. Há uma exceção para que estes funcionários possam utilizar sistemas de desbloqueio por reconhecimento facial dos seus dispositivos pessoais, como celulares.<br><br>Na cidade de Alameda, há também duas outras exceções, que não ensejariam uma violação à proibição:<br>1- Nos casos em que o funcionário tenha recebido dados obtidos por meio de sistemas de reconhecimento facial sem tê-los requisitado ou solicitado;<br>2- Quando o dado serve de evidência para alguma investigação criminal em andamento, desde que não tenha sido obtido por nenhum órgão ou funcionário público da cidade.<br><br>No caso do Projeto de Lei proposto para o Estado de Massachusetts, há a possibilidade de exceções, que serão autorizadas mediante requisição. Estas deverão descrever quais entidades serão autorizadas, o propósito de cada uso e quais aplicações serão expressamente proibidas; os protocolos de uso e gestão dos dados obtidos por meio dos sistemas de reconhecimento facial, incluindo a determinação de seu período de retenção; requerimentos de auditoria para garantir a acurácia do sistema, incluindo taxas de acurácia por gênero, raça e idade; proteções rigorosas ao devido processo legal, à privacidade, à liberdade de expressão e de associação, bem como à igualdade de gênero, raça e de religião; e mecanismos que garantam o compliance. |
| | Quais são os protocolos de uso desses sistemas? | Nos casos em que a regulação não considera como violação o recebimento de dados não solicitados, há uma determinação para que sejam deletados imediatamente, bem como uma proibição de seu uso como instrumento de prova em investigações criminais. Esses recebimentos deverão ser registrados e comunicados em um relatório anual sobre vigilância. Quaisquer evidências, prisões ou mandados de busca e apreensão obtidos fundamentados em dados dos sistemas de reconhecimento facial deverão ser considerados como violação à IVª Emenda da Constituição dos EUA.<br><br>Alguns casos também deixam claro que os sistemas de reconhecimento facial não podem ser implementados em câmeras de vigilância, veículos aéreos não-tripulados, câmeras corporais, iluminação pública e luzes de trânsito. |
| Transparência | Existe alguma previsão de política de transparência e comunicação aos cidadãos sobre o uso dos sistemas de reconhecimento facial? | |
| Segurança | Existe algum incentivo para a utilização de medidas técnicas para a proteção dos dados coletados pelos sistemas de reconhecimento facial? | O projeto de lei proposto pelo Estado de Massachusetts determina que os usos excepcionais que forem autorizados devem apresentar detalhes sobre registros de acesso e compartilhamento dos dados obtidos por meio dos sistemas de reconhecimento facial. |
| | Existe alguma disposição expressa sobre o período de retenção desses mesmos dados? | O projeto de lei proposto pelo Estado de Massachusetts determina que os usos excepcionais que forem autorizados devem apresentar detalhes sobre o período de retenção dos dados obtidos por meio dos sistemas de reconhecimento facial. |
| Não-discriminação | Existe algum cuidado ou menção sobre o risco de viés social no uso de sistemas de reconhecimento facial? | As regulações que proibem o uso dos sistemas de reconhecimento facial também apresentam como fundamento a alegação de que essa tecnologia já demonstrou falhas, como a apresentação de muitos falsos positivos na identificação de mulheres, jovens e pessoas não-brancas, de modo que exarcerbam desigualdades pré-existentes. Além disso, há uma atenção especial para o fato de que seu uso pode impactar ainda mais os direitos e liberdades civis de pessoas que vivem em áreas com alto policiamento. |
| | Existe a previsão da realização de avaliações de impacto social desses mesmos sistemas? | O projeto de lei proposto pelo Estado de Massachusetts determina que os usos excepcionais que forem autorizados devem mostrar seus níveis de acurácia para recortes de gênero, raça e idade. |

# *FRANÇA*

A França ainda não possui um marco regulatório para os sistemas de reconhecimento facial. Contudo, isso não vem impedindo os órgãos públicos do país de implementar uma série de pilotos que utilizam a tecnologia. Testes como o que foi realizado na cidade de Nice, durante o Carnaval de 2019, que contou com a participação de voluntários civis, tornam-se notórios e contribuem para a atual discussão sobre o tema no território francês[12].

Tal como o Reino Unido, a França crê que o arcabouço legal do país possui alguns instrumentos que auxiliam no enquadramento do uso dos sistemas de reconhecimento facial, ainda que não exista um instrumento específico. A diferença é que os experimentos com a tecnologia apontam para a necessidade de um marco específico, indicando que a atual abordagem no país continuará sendo a realização de testes controlados para compreender as características e os impactos do emprego de sistemas de reconhecimento facial.

Na prática, cada uso deve ser previamente autorizado por um decreto do Conselho de Estado, com opinião favorável da Comissão Nacional de Informática e Liberdade. Essas autorizações levam em consideração as particularidades de cada nova implementação. Isso significa que cada piloto autorizado funciona como um teste e uma oportunidade de debate, caminhando assim para uma futura regulação.

A tabela abaixo mostra como a cautelosa tendência francesa leva em consideração os princípios que nos servem como base de análise. Os documentos examinados foram:

- CNIL - Facial recognition: for a debate living up to the challenges;
- Parliamentary Office for Scientific and Technological Assessment - Briefing 14 - Facial Recognition - 2019.

12 VILLE DE NICE. Jun. (2019). *Rapport: Experimentation Reconnaissance Faciale*. Disponível em: https://assets.documentcloud.org/documents/6350838/Bilan-Reconnaissance-Faciale.pdf

## **Tabela 3.** França

| | | |
|---|---|---|
| Finalidade | Como os documentos e legislações analisados justificam a regulação dos sistemas de reconhecimento facial? | Os documentos franceses mencionam que já existe um enquadramento legal para uso de sistemas de reconhecimento facial no país, ainda que estes não tratem especificamente sobre o tema. Contudo, qualquer tratamento de dados biométricos por parte do Estado só poderá acontecer mediante salvaguardas apropriadas aos direitos e liberdades dos seus titulares, e somente com a finalidade de proteger seus interesses vitais ou de outros indivíduos.<br><br>Existe ainda a conclusão de que a legislação existente é insuficiente para lidar com as complexidades apresentadas pelos sistemas de reconhecimento facial. É preciso realizar testes e avaliações de impacto para se elaborar um mecanismo regulatório apropriado. De fato, o governo francês reconhece que existem propósitos legais e legítimos para o uso desses sistemas, mas que estes não devem ser considerados desejáveis e possíveis em todos os casos. |
| | Há alguma menção expressa sobre as finalidades autorizadas ou proibidas? | O governo francês reconhece o risco da vigilância em massa, apresentada pelos sistemas de reconhecimento facial, de modo que seu usos e testes só serão permitidos mediante autorização específica, a partir da avaliação das suas finalidades. Essa medida tem como objetivo preservar o anonimato em espaços públicos; as liberdades individuais, incluindo o direito à privacidade e proteção de dados, a liberdade de expressão e associação, o direito à manifestação, a liberdade de consciência e liberdade de religião. |
| Necessidade | Quais são os limites impostos aos sistemas de reconhecimento facial? | O processamento de dados biométricos sem consentimento do titular é uma exceção. Assim cada modalidade de tratamento que não permita a obtenção de consentimento deverá ser autorizada previamente. Cada uso tem suas próprias questões, sendo que algumas delas implicarão na necessidade de limites mais rigorosos. Há contudo, uma proibição já consolidada, que diz respeito ao uso de sistemas de reconhecimento facial para autenticar o acesso de crianças às escolas. |
| | Quais são os protocolos de uso desses sistemas? | |
| Transparência | Existe alguma previsão de política de transparência e comunicação aos cidadãos sobre o uso dos sistemas de reconhecimento facial? | A regulação existente recomenda a adoção de alguma forma de interação que alerte as pessoas sobre a existência de sistemas de reconhecimento facial em uso, lembrando-as das consequencias de suas interações com ferramentas digitais e dando-lhes oportunidade para afirmar seus direitos. |
| Segurança | Existe algum incentivo para a utilização de medidas técnicas para a proteção dos dados coletados pelos sistemas de reconhecimento facial? | A regulação ressalta a importância crucial de técnicas de proteção dos dados biométricos coletados e utilizados por sistemas de reconhecimento facial, tendo em vista sua sensibilidade.<br><br>Ele recomenda o armazenamento em dispositivos pessoais acessíveis apenas ao usuário, ao invés de uma base de dados central. |
| | Existe alguma disposição expressa sobre o período de retenção desses mesmos dados? | |
| Não-discriminação | Existe algum cuidado ou menção sobre o risco de viés social no uso de sistemas de reconhecimento facial? | A regulação alerta para os vieses já identificados em sistemas de reconhecimento facial, argumentando que as taxas de erro costumam ser maiores quando gênero e cor de pele são levados em consideração. |
| | Existe a previsão da realização de avaliações de impacto social desses mesmos sistemas? | |

# 4. O CENÁRIO BRASILEIRO

[contribuição do Data Privacy Brasil Research]

A implementação da tecnologia de Reconhecimento Facial pelo setor público no Brasil também tem sido acompanhada pela formação de uma efervescente arena regulatória.

Diferentemente do Reino Unido, por exemplo, no Brasil, a implementação dos sistemas de reconhecimento racial pelo setor público tem sido acompanhada por iniciativas de regulação específicas. Cabe avaliar se essas iniciativas vão no sentido de cercear o emprego da tecnologia, como é o caso dos Estados Unidos, ou de estabelecer critérios e balizas para o seu bom uso.

No ano de 2018, com a divulgação de uma série de iniciativas de emprego do reconhecimento facial no país, especialmente na área da Segurança Pública[13], foram realizadas Audiências Públicas em órgãos como a Câmara dos Deputados[14] e o Ministério Público do Distrito Federal e Territórios[15] onde ficou clara uma abertura à discussão sobre a regulamentação da prática. Nestas ocasiões, a tônica do debate centrou-se na necessidade de uma regulação ''equilibrada", com respeito a direitos fundamentais, dentre os quais à privacidade e o direito à informação. Dentre diversos pontos levantados, destacam-se sugestões, por parte dos *stakeholders* convidados para os eventos, de sistemas auditáveis, bem como de diferentes propostas de colaboração entre setores público e privado.

Hoje, não há, a nível federal, legislação específica sobre o tema. A despeito disso, o país conta com normas robustas de garantia e proteção de direitos individuais, que vão desde a Constituição até a Lei Geral de Proteção de Dados (LGPD), passando pelo Código de Defesa do Consumidor (CDC). A LGPD, aprovada em agosto de 2018, traz 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.

No caso de atividades relacionadas à segurança pública, excetuadas da lei pelo art. 4º, III, os princípios da LGPD seguem aplicáveis, pois o §1º do mesmo artigo determina que deverá haver lei específica para reger estas atividades e que seus princípios deverão ser os mesmos da LGPD. Dessa forma, é possível afirmar que princípios com os quais trabalhamos neste documento, finalidade, necessidade, transparência, segurança e não-discriminação, assim como todos os outros, poderão ser calibrados para o cenário específico de emprego de reconhecimento facial pelo poder público, inclusive em contextos de segurança pública.

A LGPD, antes de tudo, é uma regulação de riscos. Isso porque, além de garantir direitos e prescrever princípios, ela traz dispositivos voltados aos controladores de dados pessoais para que documentem suas atividades, prestem contas e também calibra sanções de acordo com o nível das medidas de prevenção ao risco adotadas previamente. Por fim, trabalha com a ideia de Relatórios de Impacto à Proteção de Dados, que, embora não sejam obrigatórios, são altamente recomendáveis e podem servir

13 O Instituto Igarapé publicou infográfico em que identifica 48 casos publicamente reportados de implementação de reconhecimento facial no Brasil desde 2011.

14 O link com o vídeo e todas as contribuições à Audiência Pública pode ser acessado aqui: <https://edemocracia.camara.leg.br/audiencias/sala/840>. Acesso em 06 de setembro de 2019.

15 Mais informações sobre a audiência: <http://www.mpdft.mp.br/portal/index.php/comunicacao-menu/sala-de-imprensa/noticias/noticias-2019/10779-mpdft-audiencia-publica-debate-uso-ferramentas-de-reconhecimento-facial>. Acesso em 07 de setembro de 2019.

de inspiração para a prática de documentação e análise de risco pelos agentes envolvidos no ecossistema do reconhecimento facial.

Se não há legislação vigente específica sobre o tema, o mesmo não se pode dizer de propostas legislativas que hoje tramitam na Câmara e no Senado. A busca por projetos de lei teve como critério de levantamento propostas cujo objeto fosse especificamente reconhecimento facial e, para os fins deste documento, foram retirados os projetos já arquivados e aqueles que fogem ao escopo de atuação do poder público. Como resultado, restaram três propostas legislativas[16], sendo uma geral[17] e duas relativas à implantação do reconhecimento facial em contextos específicos[18].

O primeiro achado interessante é que ambos os projetos voltados a setores específicos - um para controle de fluxos no transporte público e outro para identificação em estabelecimentos penais - têm como finalidade a autenticação, e não a identificação. Significa dizer que os projetos de lei federais sobre reconhecimento facial no Brasil estão interessados na pergunta ‘’Você é quem afirma ser?” e, por consequência, têm uma aplicação do reconhecimento facial limitada no espaço. Trata-se de comparar duas imagens para verificar se se trata de uma mesma pessoa, sem a necessidade de formação de grandes bancos de dados. A segunda observação é que estes projetos se limitam a prever a implantação dos sistemas de reconhecimento facial, especificamente em meios de transporte coletivos e estabelecimentos penais, sem nenhuma menção a princípios e direitos, nem a medidas de transparência, prestação de contas, documentação, ou qualquer elemento de análise de risco.

A exceção a esta lógica é o projeto de lei 4612/2019, do deputado Bibo Nunes (PSL/RS), uma vez que busca criar uma regulação geral para reconhecimento facial. Isso porque ele parte do pressuposto de que o emprego dos sistemas de reconhecimento facial, seja pelo setor privado ou público, impõe riscos que devem ser levados em consideração e, em contrapartida a estes riscos, traz algumas boas práticas relevantes: (i) previsão de direitos/preceitos; (ii) definição multissetorial de boas práticas, especialmente em casos nos quais as consequências do uso do reconhecimento facial sejam desconhecidas; (iii) obrigações específicas para desenvolvedores e utilizadores de reconhecimento facial; (iv) restrições ao uso compartilhado de dados provenientes de reconhecimento facial; (v) envolvimento da Autoridade Nacional de Proteção de Dados.

Na esfera estadual, foram identificadas quatro leis que tratam especificamente de reconhecimento facial.

Em duas delas - Lei nº 16.873/2019, do estado do Ceará e Lei nº 7.123/2015, do estado do Rio de Janeiro - fica clara a finalidade de autenticação da implantação dos sistemas de reconhecimento facial, na medida em que são atrelados a um cadastro para fins de controle de acesso a um determinado espaço (no caso, estádio de futebol e veículo de transporte público coletivo).

Nas outras duas - Lei nº 21.737/2015, do estado de Minas Gerais e Lei nº 8.113/2019, do estado de Alagoas - a previsão é genérica, para implantação de ‘’sistemas de reconhecimento facial” em estádios de futebol, podendo, na prática, ser utilizada com finalidade de autenticação ou identificação. Isto é, assim como o reconhecimento facial pode ser utilizado para validar o acesso ao estádio, também poderia ser utilizado para identificar uma ou mais faces dentre as milhares que frequentam estes espaços, sendo o principal objetivo deste emprego a segurança.

16 PL 4612/2019, PL 9414/2017 e PL 9736/2018

17 PL 4612/2019

18 PL 9414/2017 e PL 9736/2018

Apenas no caso do Rio de Janeiro há menção a direitos individuais e sanções para violação a estes direitos. Nos outros três casos, não há previsão detalhada e análise dos eventuais riscos que o emprego destas tecnologias podem implicar, na medida em que não preveem a garantia de direitos aos indivíduos afetados pelas tecnologias e nem medidas relacionadas à transparência, prestação de contas, documentação e relatórios de impacto.

Os projetos de lei estaduais também trazem novidades em relação às propostas de nível federal. A investigação em todas as assembleias legislativas, que obedeceu aos mesmos critérios dos PLs no Congresso, retornou projetos de lei distribuídos em sete estados[19] da federação. Suprimindo as propostas arquivadas, restaram 14 projetos[20], em cinco estados[21]. Diferentemente do nível federal, em todos os casos de projetos de lei a nível estadual, a finalidade da implantação do reconhecimento facial é de identificação, e não autenticação. Ou seja, nos estados a implantação do reconhecimento facial objetiva responder a uma pergunta mais genérica: ‘’quem é você?”.

Ademais, nota-se um foco expressivo na utilização dos sistemas de reconhecimento facial para fins de segurança pública, seja para coibição de crimes, ou para identificação de pessoas ‘’suspeitas ou foragidas”, ou, ainda, para identificação de desaparecidos/vítimas de crimes como sequestro.

Há ainda pelo menos três projetos[22] que preveem a instalação de sistemas de reconhecimento facial em áreas comuns, sem limitação espacial, com a finalidade genérica de identificação de criminosos e aumento da segurança para a população. Em Minas Gerais e Paraná, que fazem menção a tecnologias ‘’trazidas da China”, há previsão de que, em caso de eventual desvio de finalidade, ‘’medidas adequadas” serão tomadas. Isso denota o reconhecimento de um risco no emprego da tecnologia, porém a resposta que a lei traz é genérica.

À exceção da menção à finalidade para o emprego da tecnologia em alguns casos, os PLs estaduais não preveem princípios para o uso do RF, nem fazem menção aos direitos dos titulares dos dados que serão coletados ou a salvaguardas para possíveis violações. Também não se observa uma análise de risco embutida nas proposições, que não incluem medidas como documentação, relatórios de impacto e transparência.

Esta configuração dos projetos de lei estaduais é preocupante na medida em que a finalidade de identificação, que é a comparação, ao vivo, de uma imagem obtida por câmera de segurança com uma base de imagens, tem menos precisão do que o emprego do reconhecimento facial com finalidade de autenticação, na medida em que no primeiro caso há interferências como luz, sombras, posicionamento. Além disso, diferentemente do caso da autenticação, em ambientes grandes e abertos, é mais difícil que o indivíduo tenha ciência de que sua imagem está sendo coletada e tratada e, por consequência, mais difícil que ele possa exercer um eventual direito de oposição. Os projetos, entretanto, não parecem considerar este risco inerente e não incorporam nem as medidas de prevenção mais básicas, como o estabelecimento de princípios e direitos dos cidadãos.

A tabela abaixo resume o atual cenário nacional, com as diversas abordagens enquadradas nos princípios que servem como base de análise.

---

19 Amapá, Goiás, Minas Gerais, Paraná, Rio de Janeiro, São Paulo, Santa Catarina

20 PL 1893/19, PL 391/2019-MG, PL 148/2019-PR, PL 342/2019-RJ, PL 607/2019-RJ, PL 318/2019-RJ, PL 341/2019-RJ, PL 853/2019-RJ, PL 665/2019-RJ, PL 1101/2019-RJ, PL 1033/2019-RJ, PL 865/2019-SP

21 Goiás, Minas Gerais, Paraná, Rio de Janeiro e São Paulo.

22 PL 318/2019/RJ; PL 391/2019-MG, PL 148/2019-PR.

## **Tabela 4.** Brasil

| | | |
|---|---|---|
| Finalidade | Como os documentos e legislações analisados justificam a regulação dos sistemas de reconhecimento facial? | Dentre as poucas iniciativas de regulação existentes sobre o tema no Brasil, é possível destacar que há a preocupação em regulá-las para garantir a proteção de dados contra atos de discriminação e deturpação de seus usos, além do destaque à proteção da privacidade e a defesa das liberdades dos cidadãos. Porém, existe a percepção de que os interesses do Estado precisam ser levados em consideração. Além disso, algumas iniciativas também tratam de desenvolvimento tecnológico, fundamentando-se no desenvolvimento econômico e social sustentável e inclusivo. |
| | Há alguma menção expressa sobre as finalidades autorizadas ou proibidas? | O PL 4612/2019 não busca dispor sobre fins específicos, mas sim regular o desenvolvimento, a aplicação e usos em geral, apesar de criar salvaguardas e garantias de proteção aos cidadãos.<br><br>Já o PL 9736/2018 determina que dados biométricos dos rostos de custodiados deverão ser coletados para fins de identificação criminal.<br><br>Por fim, o PL 9414/2017, diz que o reconhecimento facial deverá ser utilizado para identificar usuários de transporte público com benefícios. |
| Necessidade | Quais são os limites impostos aos sistemas de reconhecimento facial? | O PL 4612/2019, no âmbito federal, é o único que têm uma abrangência de usos mais ampla e, por consequencia, estabelece alguns limites. Ele proibe o uso de sistemas de reconhecimento facial para o estabelecimento de regime de vigilância massiva, definida como aquela exercida sem pausas e sobre toda a população de modo indiscriminado e sem restrição de local ou período. Na esfera estadual, embora os textos legais não determinem limites expressamente, há alguns que podem ser extraídos de uma leitura mais aprofundada: sigilo dos dados, vedação à comercialização, respeito a direitos fundamentais, etc. |
| | Quais são os protocolos de uso desses sistemas? | O PL 4612/2019 determina que a futura Autoridade Nacional de Proteção de Dados deverá regulamentar os dispositivos e os protocolos de uso dos sistemas de reconhecimento facial. Além disso, o mesmo PL indica que estes sistemas devem funcionar com supervisão e controle de um agente humano. Alguns PLs estaduais detalham parcialmente a forma de utilização dos sistemas, determinando onde câmeras devem ser alocadas, quem são as autoridades que podem manejá-las, etc. |
| Transparência | Existe alguma previsão de política de transparência e comunicação aos cidadãos sobre o uso dos sistemas de reconhecimento facial? | O PL 4612/2019 determina que os agentes que desenvolvem, aplicam e ou utilizam sistemas de reconhecimento facial devem ser transparentes quanto aos parâmetros para a tomada de decisão automatizada. Também deixa claro que, apesar de resguardar os segredos comerciais, estes não podem servir de justificativa para a violação de direitos. Há uma determinação para que os agentes que apliquem ou utilizem as tecnologias sinalizem o uso ou aplicação, de forma clara ou visível. Essa sinalização deve garantir que indivíduos tomem ciência do fato antes que aconteça a captura dos dados pessoais.<br><br>Por fim, os cidadãos têm direito à informações claras sobre o uso de seus dados pessoais para quaisquer atividades que envolvam sistemas de reconhecimento facial.<br><br>Nas ocasiões em que houver compartilhamento de dados pessoais para desenvolvimento, aplicação e uso das tecnologias, isso deve ser feito de modo público e transparente, com explicações a respeito das finalidades. No caso dos estados, o PL 607/2019 dispõe que deverão ser instaladas placas informando sobre a existência de câmeras de monitoramento com sistema de reconhecimento facial nos locais onde estejam instaladas. |
| Segurança | Existe algum incentivo para a utilização de medidas técnicas para a proteção dos dados coletados pelos sistemas de reconhecimento facial? | O PL 4612/2019 remete às regras de boas práticas estabelecidas na LGPD e determina que os agentes que desenvolvem, aplicam ou utilizam as tecnologias devem se submeter a equipes externas e independentes de consultoria e monitoramento, além de usar regras e sistemas que permitam a transparência quanto a infraestrutura utilizada em todas as atividades componentes da tecnologia. |
| | Existe alguma disposição expressa sobre o período de retenção desses mesmos dados? | O único projeto (ou legislação) identificado que faz menção a período de retenção de dados é o PL 607/2019, mas ele apenas remete a um prazo mínimo de 30 dias, e não a um prazo máximo. |
| Não-discriminação | Existe algum cuidado ou menção sobre o risco de viés social no uso de sistemas de reconhecimento facial? | O PL 4612/2019 tem como um dos seus pressupostos a proibição do tratamento de dados que seja discriminatório, mas não elabora como isso deverá ser feito. |
| | Existe a previsão da realização de avaliações de impacto social desses mesmos sistemas? | Não foi identificada essa previsão em nenhuma normativa ou projeto de lei. |

# 5. ABORDAGENS COMPARADAS

**Tabela 5.** Análise comparativa dos quatro casos

| | Casos analisados | | | |
|---|---|---|---|---|
| | **Reino Unido** | **EUA** | **França** | **Brasil** |
| O uso de sistemas de reconhecimento facial pelo setor público é autorizado ou proibido? | Autorizado | Proibido | Autorizado | Autorizado |
| Em que nível administrativo se dá a regulação da autorização/proibição? | Federal | Estadual e Municipal | Federal | Estadual |
| Como se dá a regulação da autorização/proibição? | Autorização ampla, regulada de modo difuso por recomendações e documentos estratégicos, buscando estabelecer limites aos usos a partir de legislações já em vigor, sobre vigilância e privacidade. | A proibição é regulada nos âmbitos municipais e estaduais, mediante a justificativa de proteção de direitos e garantias individuais. | A autorização é regulada por um órgão de âmbito federal, que a concede individualmente para cada iniciativa de emprego por órgãos públicos. | A autorização é ampla, porém vem sendo regulada nos âmbitos estaduais. |
| Pontos fortes | O Reino Unido já possui uma vasta legislação sobre o uso de tecnologias de monitoramento, construída para regular sua estrutura geral de CFTV. Essa experiência reflete uma compreensão prévia sobre a aplicação dos princípios da finalidade, necessidade, transparência, segurança e não-discriminação, que são contemplados nas normativas direcionadas ao uso dos sistemas de reconhecimento facial. | Os Estados e Municípios dos EUA que optam pela proibição dos sistemas de reconhecimento facial entendem os princípios da finalidade, necessidade, transparência, segurança e não-discriminação são incompatíveis com o estado da arte dessa tecnologia. Isso faz com que direitos e garantias fundamentais sejam protegidos, ainda que ao custo das potencialidades da tecnologia. A abordagem estadunidense também permite maior experimentação com a regulação, uma vez que cada município ou Estado pode incorporar suas particularidades. | A França adotou uma abordagem exploratória, considerando a observância dos princípios da finalidade, necessidade, transparência, segurança e não-discriminação à cada uso dos sistemas de reconhecimento facial. A existência de um órgão central, responsável por autorizar e fiscalizar as experimentações, permite uma compreensão maior dos impactos dessa tecnologia. | Assim como ocorre nos EUA, o Brasil vem optando por uma regulação nos âmbitos estaduais. Isso permite maior experimentação e garante que os entes federativos incorporem suas particularidades na observância dos princípios. |
| Pontos fracos | A ausência de uma regulação específica para sistemas de reconhecimento facial torna mais difícil o enforcement dos princípios, tendo em vista que essa tecnologia possui particularidades que não são contempladas pela regulação de outras ferramentas de monitoramento. | A abordagem federalista reflete uma dificuldade em estabelecer uma regulação comum, que contemple todos os interesses envolvidos. | Trata-se de uma abordagem lenta, ainda que cautelosa. Conforme a demanda pelo emprego dos sistemas de reconhecimento facial aumentar, a necessidade de uma regulação específica vai se fazer presente. | A ausência de uma legislação única, ou de um órgão central que faça a fiscalização do emprego dos sistemas de reconhecimento facial dificulta a observância dos princípios, de modo que violações a direitos e garantias individuais possam ocorrer sem a devida responsabilização. |

Quando analisamos cada uma dessas abordagens lado a lado, é possível compreender os pontos fortes e fracos de cada uma, além de observarmos onde o Brasil se insere neste panorama.

O que existe hoje é a ausência de uma regulação ou orientação de alcance geral, que resulta na autorização tácita do uso de sistemas de reconhecimento facial. Essa lacuna fez com que alguns Estados tomassem a dianteira para regular o emprego da tecnologia por órgãos do setor público. Assim, o Brasil tem hoje um cenário semelhante ao dos EUA, ainda que em uma direção oposta, na qual o uso é autorizado e as regulações se dão abaixo do âmbito federal.

Tal cenário poderia ser positivo caso houvesse alguma autoridade central, como ocorre na abordagem francesa, para fiscalizar as experiências estaduais de regulação. No entanto, na ausência de um órgão central - como pode vir a ser a Agência Nacional de Proteção de Dados, por exemplo - a abordagem brasileira oferece poucas garantias para coibir os potenciais riscos aos direitos e garantias individuais gerados pelo emprego de sistemas de reconhecimento facial. Ainda que o país tenha se esforçado para construir sua Lei Geral de Proteção de Dados, é fundamental buscar a instrumentalização dos princípios nela apresentados.

# CONSIDERAÇÕES FINAIS

Regular o emprego de qualquer tecnologia emergente é complexo. Trata-se de um esforço que deve buscar o difícil equilíbrio entre preservar direitos civis e, ao mesmo tempo, permitir que a sociedade possa usufruir das transformações positivas da inovação. Tudo isso em um contexto no qual ainda não se conhece todos os possíveis impactos daquela tecnologia. Quando a regulação diz respeito ao uso de tecnologias emergentes por parte do setor público, o desafio é ainda maior, porque estamos tratando de instituições diretamente responsáveis pela preservação do interesse da sociedade.

É nesta encruzilhada que o Brasil e o mundo se encontram atualmente, quando pensamos na regulação do emprego de sistemas de reconhecimento facial pelo setor público. Mesmo em países como o Reino Unido, com uma longa história de utilização de tecnologias de videomonitoramento, os esforços de regulação ainda estão no começo.

O que pode ser aprendido ao olharmos as tendências internacionais de regulação dos sistemas de reconhecimento facial é o exercício da cautela. Os três países analisados neste documento reconhecem que essa tecnologia é potencialmente perigosa, de modo que sua capacidade não pode se sobrepor aos riscos já identificados. Seu uso massivo deve ser dissuadido e é preciso sempre refletir a respeito da adoção de soluções menos arriscadas, de uso mais consolidado.

Da mesma forma que o emprego apressado oferece riscos, qualquer iniciativa de regulação dos sistemas de reconhecimento facial que se pautem pela urgência também pode ter resultados problemáticos. Primeiramente, é preciso se esforçar para pensar em regulações que sejam tecnologicamente neutras. O reconhecimento facial é apenas uma das modalidades de tecnologia de identificação de pessoas que funcionam a partir do processamento de dados biométricos - informações baseadas em características fisiológicas e comportamentais

de um indivíduo, tais como sua fisionomia, impressões digitais e padrão da retina ocular - e do monitoramento por vídeo. Ocupando essa mesma categoria existem outras tecnologias, como o reconhecimento de linguagem corporal e a detecção de padrões térmicos. Isso significa que uma regulação eficiente precisa considerar as rápidas mudanças na tecnologia, buscando antecipar essas novas aplicações e funcionalidades.

Em segundo lugar, a regulação deve ser precedida de um amplo debate público, travado de modo acessível e transparente. Somente assim será possível criar instrumentos regulatórios que contemplem a perspectiva de especialistas e de todos os grupos potencialmente afetados pelo emprego da tecnologia, garantindo assim a proteção de dados e a elaboração de estratégias para mensurar impactos.

Finalmente, a análise apresentada neste documento nos traz uma importante lição. Se por um lado estamos diante de um novo desafio, trazido pela necessidade de regular uma tecnologia emergente, por outro, esse desafio não é enfrentado em um vácuo normativo. Reino Unido, Estados Unidos e França possuem legislações e jurisprudências sobre a proteção de dados pessoais, que servem como um importante guia para a regulação de qualquer tecnologia de processamento de dados biométricos. No Brasil, a Lei Geral de Proteção de Dados (LGPD), que ainda aguarda a sua entrada em vigor, traz princípios e parâmetros balizadores para a aplicação de sistemas de reconhecimento facial no país. Mesmo que a lei não se aplique totalmente para os tratamentos de dados pessoais com fins de segurança pública, defesa nacional e segurança do Estado, ela deixa claro que os princípios da proteção de dados deverão ser observados em absolutamente todos os casos.

Assim, qualquer legislador ou gestor público interessado na regulação dos sistemas de reconhecimento facial no Brasil tem nos princípios gerais da LGPD o ponto de partida para pensar em instrumentos eficazes e observantes das garantias individuais.

INSTITUTO IGARAPÉ
a think and do tank

Instituto Igarapé é um think and do tank independente, dedicado à integração das agendas de segurança, clima e desenvolvimento. Nosso objetivo é propor soluções e parcerias a desafios globais por meio de pesquisas, novas tecnologias, influência em políticas públicas e comunicação. Somos uma instituição sem fins lucrativos, independente e apartidária, com sede no Rio de Janeiro, mas cuja atuação transcende fronteiras locais, nacionais e regionais.

Instituição parceira

DataPrivacyBR RESEARCH

A Associação de Pesquisa Data Privacy Brasil Research produz pesquisas e ações de incidência na intersecção entre tecnologias, uso de dados e direitos fundamentais. A associação desenvolve projetos estratégicos de pesquisa em proteção de dados pessoais, mobilizando conhecimentos que podem ajudar reguladores, juízes e profissionais do direito a lidar com questões complexas que exigem conhecimento profundo sobre como os sistemas sócio técnicos afetam os direitos fundamentais.

**Instituto Igarapé**

Rio de Janeiro - RJ - Brasil
Tel/Fax: +55 (21) 3496-2114
contato@igarape.org.br
facebook.com/institutoigarape
twitter.com/igarape_org

**www.igarape.org.br**

**Direção criativa e layout**

Raphael Durão - STORMdesign.com.br

ISSN 2359-0998

INSTITUTO IGARAPÉ
a think and do tank

**www.igarape.org.br**