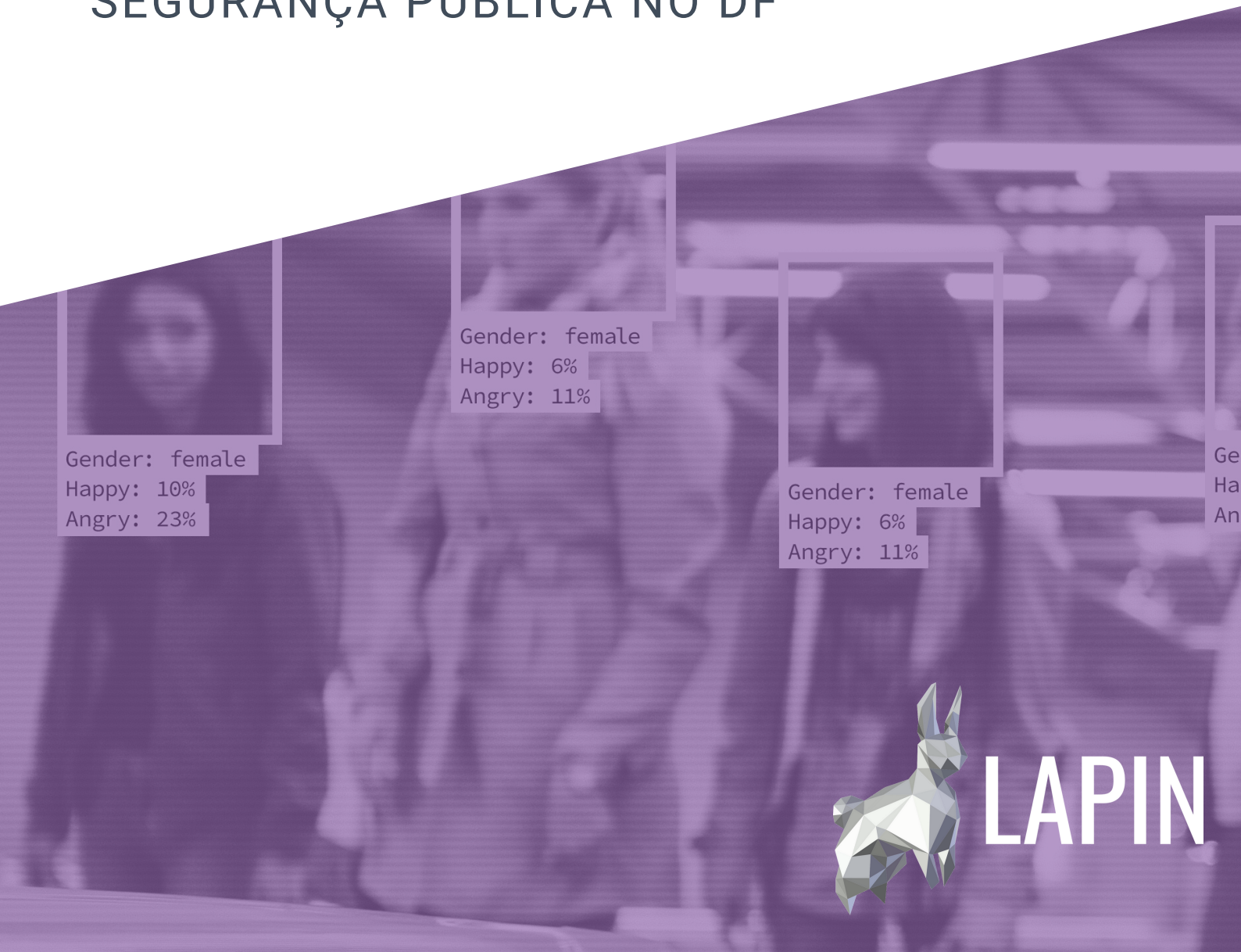
2021 | FEVEREIRO

NOTA TÉCNICA

LEI 6.712/20

10 RECOMENDAÇÕES PARA O USO DE RECONHECIMENTO FACIAL PARA SEGURANÇA PÚBLICA NO DF



LAPIN

Realização:

Laboratório de Políticas Públicas e Internet - LAPIN

Autoria:

Carolina Reis

Revisão:

Amanda Espiñeira

José Renato Laranjeira de Pereira

Thiago Guimarães Moraes

Imagem de Capa:

Izusek, Getty Images Signature

LAPIN
LABORATÓRIO DE POLÍTICAS PÚBLICAS E INTERNET

lapin.org.br
@lapin.br
/lapinbr
/lapinbr

Sobre esta nota técnica

A Lei Distrital nº 6.712/2020, que estabeleceu as condições para o **uso de tecnologia de reconhecimento facial para fins de segurança pública no Distrito Federal**, traz diretrizes para a implementação da tecnologia no setor, o que já ocorre amplamente em outras unidades federativas sem a devida regulamentação.

No entanto, a Lei possui alguns pontos de preocupação, especialmente no que diz respeito à clareza dos critérios e condições de utilização da tecnologia para segurança pública; medidas de segurança para a proteção dos dados coletados; e mecanismos de transparência e auditoria.

Considerando os danos à privacidade e à proteção de dados que a tecnologia de reconhecimento facial pode causar, o **Laboratório de Políticas Públicas e Internet – LAPIN** editou esta nota técnica para apresentar suas considerações sobre o tema.

Quem somos nós

O Laboratório de Políticas Públicas e Internet (LAPIN) é um *think tank* de composição multidisciplinar com sede na capital federal brasileira. Seu objetivo é apoiar o desenvolvimento de políticas públicas voltadas para a regulação das tecnologias digitais por meio da pesquisa e da conscientização da sociedade.

SUMÁRIO

I - Introdução 5

II - O contexto da implementação de tecnologias de reconhecimento facial para a segurança pública no Brasil 8

III - Como a Lei Distrital nº 6.712/2020 inova, mas também acende alertas 10

IV - As matérias ausentes na Lei Distrital nº 6.712/2020 20

V - Resumo de recomendações para a Lei Distrital nº 6.712/2020 24

VI - Conclusão 31

Anexo: tabela com recomendações 32

I - Introdução

A Lei Distrital nº 6.712/2020 foi editada num momento em que o uso de tecnologias de reconhecimento facial (TRF) para segurança pública está no centro do debate público. A implementação desses sistemas já ocorre em diversos estados da federação num contexto de **vazio normativo** dada a inexistência de uma lei federal que regule a proteção de dados para segurança pública. Isso se reflete na ausência de leis, federais ou estaduais, que regulem o uso de TRF em espaços públicos com fins de prevenção e persecução penal[1], bem como guias e recomendações de autoridades reguladoras.

Neste sentido, a Lei Distrital inova ao regulamentar seu uso para segurança pública sem vincular a espaços determinados e ao definir como deve ocorrer sua implementação. Além disso, seu texto contém **aspectos positivos** que podem ser observados futuramente em leis similares que vierem a ser desenvolvidas sobre o tema.

Entretanto, o texto da Lei contém **pontos preocupantes** que devem ser considerados na edição de um futuro decreto regulamentador a ser elaborado pelo governo do Distrito Federal, de modo a proteger as liberdades e direitos de indivíduos em seu território, principalmente sob a perspectiva da privacidade e da proteção de dados pessoais.

A presente nota técnica tem por objetivo discutir os aspectos positivos e negativos da Lei Distrital nº 6.712/2020 e **propor medidas que a adequem** às exigências do sistema

[1] De acordo com levantamento feito por pesquisadores do Instituto Igarapé e do Data Privacy Brasil, de junho de 2020, havia leis em quatro estados que se referiam à TRF. Duas delas - a Lei nº 16.873/2019, do Ceará, e a Lei nº 7.123/2015, do Rio de Janeiro - tem por finalidade a autenticação de indivíduos respectivamente em catracas de estádios e arenas desportivas estaduais e no sistema intermunicipal de transporte rodoviário. Outras duas - a Lei nº 21.737/2015, de Minas Gerais e a Lei nº 8.113/2019, de Alagoas - limitam o uso da tecnologia a estádios de futebol. O relatório indicou, ainda, três projetos de lei estaduais referentes ao uso de TRF em áreas comuns não especificadas para fins de segurança pública. São eles os PLs 391/2019, de Minas Gerais; 318/2019, do Rio de Janeiro; e 148/2019, do Paraná. Tais projetos, segundo busca feita pelo LAPIN nos sítios eletrônicos das respectivas Assembleias Legislativas em dezembro de 2020, seguem em tramitação. Para mais detalhes, ver: Pedro Augusto P. Francisco, Louise Marie Hurel, e Mariana Marques Rielli, "Regulação do reconhecimento facial no setor público: avaliação de experiências internacionais" (Instituto Igarapé, Data Privacy Brasil, junho de 2020), https://igarape.org.br/wp-content/uploads/2020/06/2020-06-09-Regula%C3%A7%C3%A3o-do-reconhecimento-facial-no-setor-p%C3%BAblico.pdf.

jurídico brasileiro, em especial ao exercício do **direito à proteção de dados,** cuja natureza de direito fundamental foi determinada pelo Supremo Tribunal Federal no âmbito da Ação Direta de Inconstitucionalidade nº 6.387. Ademais, a nota utiliza como fonte não apenas as obrigações legais brasileiras, mas também boas práticas propostas e utilizadas no plano internacional.

Este documento está **dividido em três capítulos**. O primeiro deles apresenta, de forma breve, o cenário em que a Lei Distrital foi elaborada; o segundo discute os pontos fortes e insuficientes da Lei, bem como as propostas para aprimorá-los; e o terceiro traz recomendações de forma direta e esquematizada. Em **anexo**, encontra-se uma tabela com as recomendações, divididas de acordo com a referência delas na Lei, para melhor visualização.

As **recomendações** propostas por esta nota técnica estão listadas, de forma condensada, a seguir[2]:

1. Utilizar tecnologias de reconhecimento facial apenas em casos excepcionais, determinados, envolvendo investigações específicas e para procurar indivíduos já identificados, a fim de evitar a normalização e a vigilância em larga escala;
2. Definir os conceitos de espaços e equipamentos públicos e restringir o uso da tecnologia em áreas próximas a organizações religiosas, políticas, de tratamento de saúde ou similares, de forma a evitar ao máximo a captura de dados de natureza sensível;
3. Estabelecer protocolos de atuação e abordagem a serem seguidos pelos agentes em caso de alertas emitidos pelo sistema e que possam ser consultados facilmente pela população;
4. Definir critérios para utilização da tecnologia, tais como delimitar que seu uso seja feito exclusivamente para investigação de crimes de natureza grave, adotar mecanismos para minimizar o número de pessoas sujeitas a seu escrutínio e determinar o período máximo de aplicação, não ultrapassando 72h em nenhum caso;

[2] No anexo, é possível encontrar a lista expandida de recomendações.

5. Instituir protocolos de controle de acesso aos dados oriundos do sistema que restrinjam o tratamento de dados pessoais somente a pessoas que realmente necessitem acessar esses dados e registrem todos os acessos realizados;
6. Identificar as bases de dados utilizadas como fonte para o pareamento de imagens analisadas pelo sistema e informá-las à sociedade;
7. Estipular categorias de dados pessoais, definir tempos de armazenamento distintos de acordo com a sua natureza, não ultrapassando 6 meses em qualquer hipótese, e estabelecer diretrizes para o compartilhamento de dados;
8. Adotar medidas de segurança e de proteção de dados, inclusive pseudonimização;
9. Instaurar procedimentos para o exercício de direitos do titular dos dados;
10. Elaborar Relatório de Impacto à Proteção de Dados antes da implementação da tecnologia e divulgar relatórios de transparência, de forma periódica, que contenham informações acerca do uso e dos resultados da tecnologia.

II - O contexto da implementação de tecnologias de reconhecimento facial para a segurança pública no Brasil

O combate à violência urbana no Brasil tem sido prioridade de governos em diferentes níveis federativos e espectros políticos. Considera-se, inclusive, que a posição de agentes públicos é de que qualquer medida capaz de auxiliar neste propósito deve ser implementada, com pouca ou nenhuma análise sobre todos os riscos de sua utilização[3].

Essa postura não é diferente com sistemas de reconhecimento facial. Considerando as vantagens que a tecnologia promete, inclusive de custos mais baixos, maior número e qualidade de resultados e realocação de recursos humanos, sua implementação para fins de segurança pública tem se expandido no país[4].

Um dos riscos inerentes à utilização de tecnologia de reconhecimento facial (TRF) é o de violação do direito à proteção de dados. A regulação do direito no Brasil se dá majoritariamente pela Lei Geral de Proteção de Dados (LGPD). Apesar de seu alcance para segurança pública ser limitado, conforme expresso no art. 4º, §1º[5], seus princípios e os direitos previstos ao titular se aplicam ainda a essa finalidade.

---

[3] Renato Sérgio de Lima, Samira Bueno, e Guaracy Mingardi, "Estado, polícias e segurança pública no Brasil", *Revista Direito GV* 12, nº 1 (abril de 2016): 49–85, https://doi.org/10.1590/2317-6172201603.

[4] Primeiramente utilizada no contexto dos grandes eventos esportivos no país, como a Copa do Mundo de Futebol Masculino em 2014 e as Olimpíadas em 2016, a tecnologia tem sido adotada como prática recorrente para fins de segurança pública em diversos estados do país, como Bahia, Ceará, São Paulo, Rio de Janeiro e Distrito Federal. Para mais informações, ver: Instituto Igarapé, "Infográfico: Reconhecimento facial no Brasil", https://igarape.org.br/infografico-reconhecimento-facial-no-brasil/.

[5] Art. 4º Esta Lei não se aplica ao tratamento de dados pessoais:
(...)
III - realizado para fins exclusivos de:
a) segurança pública;
(...)
§ 1º O tratamento de dados pessoais previsto no inciso III será regido por legislação específica, que deverá prever medidas proporcionais e estritamente necessárias ao atendimento do interesse público, observados o devido processo legal, os princípios gerais de proteção e os direitos do titular previstos nesta Lei.

Apesar da recente submissão do Anteprojeto de Lei de Proteção de Dados para Segurança Pública e Persecução Penal ao Presidente da Câmara dos Deputados, Rodrigo Maia, cuja redação foi elaborada por Comissão de Juristas composto por especialistas no tema[6], **até a data de publicação desta Nota, não há regulamentação da matéria com força de lei**.

Além disso, vale ressaltar que, até a promulgação da Lei Distrital nº 6.712 /2020, **nenhum ente federativo havia aprovado lei regulamentando a implementação de sistemas de reconhecimento facial em seu território**. Portanto, a implementação de TRFs para segurança pública no Brasil se dá num **vazio normativo,** em que se observa a falta de **transparência** no que concerne a critérios de uso, medidas de segurança de dados e indicadores de gestão e resultado.

[6] Marcos Urupá, "Maia recebe anteprojeto que regula tratamento de dados em investigações criminais", Teletime, 05 de novembro de 2020, https://teletime.com.br/05/11/2020/maia-recebe-anteprojeto-que-regula-tratamento-de-dados-em-investigacoes-criminais/.

III - Como a Lei Distrital nº 6.712/2020 inova, mas também acende alertas

A Lei Distrital nº 6.712/2020 é a primeira nesse nível hierárquico normativo a regulamentar a forma de implementação de TRF para segurança pública no Brasil. Com isso, ela satisfaz um importante critério no contexto do direito à proteção de dados, que é a existência de autorização legal para o uso de tecnologias de vigilância[7].

Entretanto, não basta apenas a existência formal do texto legal; é preciso que seu conteúdo esteja compatível com o ordenamento jurídico, respeitando direitos e obrigações. Este capítulo, portanto, **destaca os aspectos positivos da Lei, ao passo que também indica pontos de atenção** na redação e conceitos dos dispositivos legais.

a. Da vedação ao uso de tecnologia de reconhecimento facial para vigilância em larga escala

O art. 2º contém definições importantes[8] que vão orientar o cumprimento da Lei. Inclui-las no texto legal demonstra preocupação em não expandir seu escopo de aplicação. Contudo, **a definição do inciso II não está suficientemente precisa** e pode deixar dúvidas ou espaços não regulados quanto ao uso da tecnologia.

O inciso II do art. 2º traz o conceito de "**vigilância contínua"**, assim definido pela lei:

> *II - vigilância contínua: utilização de TRF para envolver-se em um esforço contínuo de rastreamento dos movimentos físicos de um indivíduo identificado em um ou mais locais públicos onde esses movimentos ocorrem,*

[7] Thiago Guimarães Moraes, "A spark of light in the going dark: Legal safeguards for law enforcement's encryption circumvention measures" (Master thesis, Tilburg University, 2019).

[8] Art. 2º Para os efeitos desta Lei, considera-se:
I – **tecnologia de reconhecimento facial**: a tecnologia que analisa as características faciais usada para a identificação pessoal exclusiva de indivíduos em imagens estáticas ou em vídeos;
II – **vigilância contínua**: a utilização de TRF para envolver-se em um esforço contínuo de rastreamento dos movimentos físicos de um indivíduo identificado em um ou mais locais públicos onde esses movimentos ocorrem, durante um período de tempo superior a 72 horas, seja em tempo real, seja por meio da aplicação dessa tecnologia para registros históricos.

> *durante um período de tempo superior a 72 horas, seja em tempo real, seja por meio da aplicação dessa tecnologia para registros históricos.*

Tal definição é de grande importância para a compreensão do texto legal, já que o art. 3º veda **"o uso de TRF para vigilância contínua de um indivíduo ou grupo de indivíduos em qualquer hipótese"**. Entretanto, da leitura conjunta dos dois dispositivos, não é possível depreender com clareza se a vigilância em larga escala é proibida pela Lei Distrital nº 6.712/2020.

Isto porque o inciso II do art. 2º condiciona a vigilância contínua àquela realizada em desfavor de um indivíduo identificado. Se tal premissa for interpretada juntamente ao art. 3º, a leitura poderia indicar que a vedação à vigilância contínua só é válida para indivíduo ou grupo de indivíduos definidos **quando operada por até 72h**.

Assim, numa interpretação inversa do dispositivo, a vigilância contínua de indivíduos indeterminados seria possível - o que se poderia levar justamente à vigilância em larga escala.

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 seu consentimento. A situação é ainda mais danosa se os dados coletados forem sensíveis, como são aqueles obtidos por TRF.

Considerando o uso da tecnologia em tempo real e em registros anteriormente capturados, tal vigilância pode acarretar violações às liberdades e direitos de indivíduos monitorados[9]. Isso porque a aplicação massiva dessa tecnologia pode gerar o chamado *chilling effect*, fenômeno no qual indivíduos temem exercitar o seu direito à liberdade de expressão, associação e reunião por receio de serem vigiados e

[9] Ella Jakubowska e Diego Naranjo, "Ban Biometric Mass Surveillance: A set of fundamental rights demands for the European Commission and EU Member States" (European Digital Rights (EDRi), 13 de maio de 2020); Philip Agre, "Your Face Is Not a Bar Code: Arguments Against Automatic Face Recognition in Public Places", University of California, 2003, https://pages.gseis.ucla.edu/faculty/agre/bar-code.html; Jennifer Lynch, "Face Off: Law Enforcement Use of Face Recognition Technology" (Electronic Frontier Foundation, 2020), https://www.eff.org/wp/face-off.

consequentemente punidos por suas ações[10]. Pode ocorrer, ainda, o desvirtuamento da função primária da vigilância, ou seja, a utilização dos dados obtidos para outros fins que não o de auxiliar a segurança pública[11].

O mais adequado é utilizar a tecnologia de forma excepcional, **apenas em casos determinados**, ou seja, durante investigações específicas e buscando indivíduos já tidos como suspeitos pelas autoridades, a fim de controlar melhor os efeitos negativos sobre liberdades individuais[12].

Dessa forma, a vedação do inciso II deveria ser melhor especificada, de modo a que se permita somente a vigilância contínua de indivíduos especificados, por até 72h, e não em larga escala, como pretende a norma. Logo, cabe ao decreto regulamentador sanar eventuais divergências interpretativas, para **vedar, de forma explícita, a utilização de TRF em desfavor de grupos de indivíduos indeterminados em qualquer contexto em que não houver autorização judicial para tanto**.

b. Do uso em espaços públicos

Um **aspecto importante** da Lei Distrital nº 6.712/2020 vem no art. 4º, que prevê a **restrição do uso de TRF para segurança pública a espaços e equipamentos públicos**. Por serem conceitos abrangentes e, em determinadas hipóteses, controversos, é necessário definir precisamente em quais espaços e equipamentos a tecnologia pode ser aplicada para a segurança pública.

Não está claro, por exemplo, se áreas a princípio públicas, mas concedidas à iniciativa privada, como aeroportos, estariam abarcados na definição do art. 4º. Outro exemplo

---

[10] Jonathon Penney, "Internet surveillance, regulation, and chilling effects online: a comparative case study." *Internet Policy Review*, vol. 6, ed. 2, 2017. Disponível em: https://policyreview.info/articles/analysis/internet-surveillance-regulation-and-chilling-effects-online-comparative-case. Acesso em: 14 de nov. 2020.

[11] A tese de doutorado de Bruno Cardoso sobre a utilização de câmeras de vigilância pela polícia militar na cidade do Rio de Janeiro já trazia indícios de como as imagens, ainda sem TRF à época, eram usadas para outros propósitos que não a segurança pública. A título de exemplo, os policiais encarregados usualmente aproveitavam as câmeras para fins pessoais. Para mais, ver: Bruno Cardoso, "Todos os Olhos. Videovigilâncias, videovoyeurismos e (re)produção imagética na tecnologia digital" (Doctoral dissertation, 2010), http://rgdoi.net/10.13140/RG.2.2.30552.19209.

[12] Clare Garvie et al., "The Perpetual Line-Up: Unregulated Police Face Recognition in America" (Georgetown Law: Center on Privacy & Technology, 18 de outubro de 2016).

seriam escolas ou hospitais públicos, cujos frequentadores, respectivamente, são incapazes ou podem estar em situação de vulnerabilidade.

Se bem determinados os conceitos de espaços e equipamentos públicos, é possível reduzir a coleta de dados pessoais sensíveis e de cunho íntimo se, adicionalmente, incluírem-se restrições à utilização da tecnologia em áreas próximas a hospitais ou clínicas médicas, sindicatos, diretórios partidários, recintos religiosos e outros espaços similares.

Assim, **reduz-se a coleta de dados sensíveis** como os de convicção religiosa, opinião política, filiação sindical ou a organização de caráter religioso, filosófico ou político, ou, ainda, referente à saúde ou à vida sexual[13].

O parágrafo único do art. 4º ainda traz a **obrigação de fixação de placas informando o uso de TRF** nos locais em que a tecnologia for usada. A medida é positiva, mas, para que essa determinação seja realmente efetiva, tais placas devem conter **informações em redação clara e acessível** e referência às identidades de controlador e encarregado, finalidades e base legal para o processamento dos dados e direitos do titular.

Além disso, a placa deve estar **em local visível e em tamanho suficiente** para que todas as informações sejam facilmente lidas. A placa deve indicar, ainda, **onde é possível encontrar mais informações a respeito** do uso da tecnologia, tanto online como em um documento físico, que deve estar disponível no próprio espaço onde o sistema opera[14]. Além disso, os documentos online e físico devem conter instruções para que o titular de dados possa exercer seus direitos previstos . A linguagem desses documentos deve ser compreensível a quaisquer níveis de instrução.

---

[13] A Universidade de Georgetown, nos Estados Unidos, fez um estudo de caso interessante sobre o uso de TRF na cidade norte-americana de Detroit. Ali, a polícia anexava imagens obtidas de câmeras privadas, instaladas em casas, lojas e outras locais privados, ao seu circuito de câmeras. O estudo demonstrou que, mais que auxiliar nas atividades de segurança, as imagens revelavam informações sensíveis sobre os transeuntes, como idas a clínicas de fertilização ou a determinados templos religiosos. O relatório do estudo, em inglês, pode ser acessado aqui: Clare Garvie e Laura M. Moy, "America under watch: Face surveillance in the United States" (Washington, DC: Georgetown Law: Center on Privacy & Technology, 16 de maio de 2019).

[14] Thiago Guimarães Moraes, Eduarda Costa Almeida, e José Renato Laranjeira de Pereira, "Smile, You Are Being Identified! Risks and Measures for the Use of Facial Recognition in (Semi-)Public Spaces", *AI and Ethics*, 10 de outubro de 2020, https://doi.org/10.1007/s43681-020-00014-3.

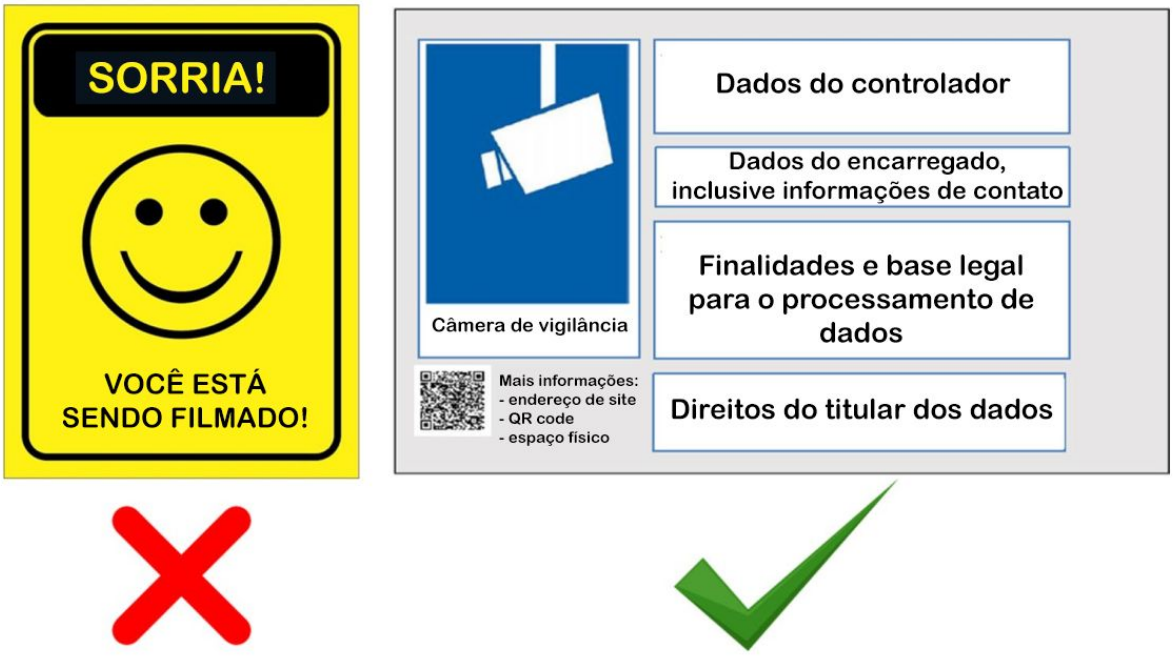


Figura 1: Sugestão de placa informativa sobre uso de TRF em espaços públicos. Adaptada de: Thiago Guimarães Moraes, Eduarda Costa Almeida, e José Renato Laranjeira de Pereira, "Smile, You Are Being Identified! Risks and Measures for the Use of Facial Recognition in (Semi-)Public Spaces", *AI and Ethics*, 10 de outubro de 2020, https://doi.org/10.1007/s43681-020-00014-3.

c. Da revisão de alertas positivos por agentes humanos

Outro ponto positivo que a Lei Distrital apresenta são as **obrigações de revisão de identificações positivas por um agente humano,** tanto no momento do alerta emitido pelo sistema quanto no momento da abordagem do indivíduo identificado. Tais exigências, contidas no art. 5º caput e parágrafo único, são importantes garantias contra os chamados falsos positivos, situações em que o sistema atribui a uma pessoa uma identidade que não corresponde àquela que ela realmente possui.

Entretanto, para que essas determinações sejam efetivas, elas devem ser complementadas com a criação de **protocolos específicos de atuação e de abordagem a serem seguidos pelos agentes** quando forem abordar indivíduos que tenham sido identificados pelo sistema de reconhecimento facial[15].

[15] Clare Garvie et al., "The Perpetual Line-Up: Unregulated Police Face Recognition in America" (Georgetown Law: Center on Privacy & Technology, 18 de outubro de 2016).

Tais protocolos devem conter instruções desde a validação do alerta positivo até a verificação da identidade da pessoa *in loco*, passando pela forma de comunicação entre agentes na central de vídeo e aqueles nos espaços públicos e entre estes e as pessoas abordadas.

Os protocolos devem, ainda, ser **amplamente divulgados e estar disponíveis**, tanto nos documentos que contém mais informações sobre as operações de uso de TRF, quanto nos portais dos órgãos envolvidos na aplicação da lei, acessíveis, com linguagem compreensível, por toda a sociedade.

d. Da coleta de dados

O art. 6º[16], por sua vez, contém uma positiva previsão que indica a preocupação com o tipo de dado pessoal coletado por tecnologias de reconhecimento facial, informando seu **caráter sensível**, "cujo **tratamento deve ser restrito a seu uso autorizado**".

Todavia, o dispositivo não traz informações acerca dos critérios para o tratamento e uso desses mesmos dados, o que pode se traduzir em incertezas sobre como deverão ser as restrições de acesso. Além disso, faltam previsões a respeito de mecanismos para garantir a segurança dos dados tratados pelo sistema.

Como já mencionado, sistemas de reconhecimento facial utilizam uma tecnologia invasiva, que captura dados biométricos de difícil modificação e que são considerados dados sensíveis nos termos da LGPD. Logo, é necessário **evitar a normalização do seu uso, autorizando-o apenas em situações excepcionais**.

Tais situações devem atender uma lista de critérios similares e ser analisadas de forma individual. Isso significa também **evitar o uso da tecnologia em tempo real**, dada a quantidade de dados pessoais excessivamente coletados A justificativa,

[16] Art. 6º As informações decorrentes do uso de TRF são dados pessoais sensíveis cujo tratamento deve ser restrito a seu uso autorizado, respeitada a Lei federal nº 13.709, de 14 de agosto de 2018.
Parágrafo único. É vedado o tratamento dos dados a que se refere esta Lei por pessoa de direito privado, exceto em procedimentos sob tutela de pessoa jurídica de direito público, que devem ser objeto de informe específico à autoridade nacional e devem observar a limitação imposta na legislação nacional.

nessas hipóteses, deve ser mais contundente que para o uso em imagens capturadas anteriormente ("registros históricos", como consta na Lei).

Considerando a inexistência de uma lei federal específica sobre o uso de TRF para fins penais, não há critérios específicos quanto a quais tipos de **investigação criminal** podem ser objeto da tecnologia[17]. Entretanto, o Distrito Federal deve editar instruções para suas polícias a fim de determinar:

- para **quais tipos penais** a TRF pode produzir provas. Recomenda-se que só se produza provas através de TRF apenas quando o fato investigado constituir infração penal de alto potencial ofensivo[18] ou considerada hedionda[19].
- **por quanto tempo** a tecnologia pode ser empregada para um determinado objetivo. Neste ponto, a Lei Distrital já indica, no art. 2º, II, o tempo máximo de 72 horas, que se apresenta razoável.
- na utilização de TRF para persecução criminal, a comprovação de existência de **indícios razoáveis da autoria ou participação** em infração penal. Nestas circunstâncias, alguns sujeitos devem ser excluídos do escrutínio da tecnologia para fins probatórios, como menores de idade.
- Na hipótese de **já haver instrução processual penal em curso**, as decisões a respeito das condições de uso de provas obtidas por meio da tecnologia dependem de determinação judicial.

Outro ponto muito relevante se refere às **bases de dados** utilizadas como fonte para o pareamento com assinaturas faciais[20] geradas pelo sistema. Por se tratar de implementação para fins de segurança pública, não se deve utilizar outras imagens que não as de **indivíduos com mandados de prisão em aberto e considerados desaparecidos**. As imagens coletadas de outras pessoas devem ser imediata e automaticamente apagadas.

---

[17] A título de exemplo, a Lei Federal nº 9.296/96 regula as hipóteses e critérios para o uso de interceptação de comunicações telefônicas como prova em investigação criminal e em instrução processual penal. Por se tratar de medida que interfere gravemente o direito à privacidade, esta só pode ocorrer mediante autorização judicial.

[18] Crimes de alto potencial ofensivo tem pena mínima superior a um ano, pena máxima superior a quatro anos e não admitem a suspensão condicional do processo ou a transação da pena. Para mais, ver: Luiz Flávio Gomes (coord), *Curso de Direito Penal - Parte Especial*, 2015, Ed. Juspodivm.

[19] Os crimes hediondos estão listados na Lei n. 8.072/90.

[20] Assinatura facial é a representação matemática do conjunto dos dados faciais de uma pessoa, gerada justamente por sistemas de reconhecimento facial.

Por outro lado, o uso de bases de dados originalmente não utilizadas em contextos criminais, como as de registros gerais (RGs) ou carteiras nacionais de habilitação (CNHs) implica em desvio de finalidade e desproporcionalidade no uso da tecnologia.

Retratos falados também devem ser vetados, uma vez que são tentativas de aproximação da realidade que perpassa, primeiramente, pela memória da vítima ou testemunha e, depois, pela interpretação e habilidade do papiloscopista[21]. Essa camada de filtros afeta significativamente a precisão da identificação do indivíduo.

Relevante, ainda, é manter a base de dados utilizada para o pareamento constantemente atualizada, a fim de evitar situações como a ocorrida no Rio de Janeiro em 2019, onde uma mulher foi incorretamente identificada como uma pessoa com um mandado de prisão em aberto. Além do caso de falso positivo, a pessoa procurada já se encontrava numa penitenciária estadual desde 2015. Isso significa que a base de dados da polícia civil estava há muito tempo desatualizada[22].

e. Do controle de acesso

Para evitar que a utilização da tecnologia seja desvirtuada, é preciso instituir um **protocolo de acesso com autorização restrita**[23] ao sistema e aos dados coletados por este. Para tanto, define-se quem pode ingressar e rodar o sistema; quem pode solicitar a aplicação da tecnologia; e quem pode ter acesso aos resultados.

Todo e qualquer acesso ao sistema deve ser registrado e conter informações como o número de matrícula do usuário, data e horário do acesso, e justificativa ou razão para tanto. Além disso, deve haver **registro de toda e qualquer extração e compartilhamento de dados** do sistema, contendo formações similares às de acesso.

---

[21] Outro estudo da Universidade de Georgetown apontou os riscos do uso de dados defeituosos em sistemas de reconhecimento facial. Via de regra, os resultados obtidos não são confiáveis e levam a erros graves. Para mais informações: Clare Garvie, "Garbage in, Garbage out: Face Recognition on Flawed Data" (Georgetown Law: Center on Privacy & Technology, 16 de maio de 2019), https://www.flawedfacedata.com.

[22] Para mais informações, ver: Antonio Werneck, "Reconhecimento facial falha em segundo dia, e mulher inocente é confundida com criminosa já presa", O Globo, 11 de julho de 2019, https://oglobo.globo.com/rio/reconhecimento-facial-falha-em-segundo-dia-mulher-inocente-confundida-com-criminosa-ja-presa-23798913.

[23] Moraes, Almeida, e de Pereira, "Smile, You Are Being Identified! Risks and Measures for the Use of Facial Recognition in (Semi-)Public Spaces".

Ademais, é importante que qualquer usuário do sistema tenha passado por um **treinamento adequado ao manuseio.** Isso inclui conhecer suas especificidades, o perfil de similaridade adotado, saber adotar as medidas de segurança necessárias, reconhecer indícios de entrada indevida e ter mecanismos de aviso e suspensão do funcionamento em caso de irregularidade [24].

f. Do compartilhamento de dados

O sétimo e último artigo da Lei Distrital traz previsões muito relevantes, mas que também devem ser analisadas com cautela. O caput do art. 7º autoriza o **compartilhamento dos dados** obtidos por TRF com outros órgãos de segurança pública brasileiros[25].

Mais uma vez, salienta-se a importância de haver protocolos e critérios para o compartilhamento, inclusive a certificação de que **o órgão receptor assegura um grau de proteção adequado** aos dados recebidos[26]. Igualmente, há necessidade de **autorização específica** para o compartilhamento, seja através de regulamentação, convênio ou contrato entre as partes[27].

Em relação ao art. 7º, §1º[28], a entidade remetente - neste caso, os órgãos de segurança do Distrito Federal - deve **assegurar a qualidade dos dados** mesmo após o compartilhamento, informando ao órgão receptor sobre correção, a eliminação, a

[24] Tais medidas estão alinhadas com o Código de Processo Penal, que estabelece, em seus art. 158-A e seguintes, a chamada *cadeia de custódia*. Como define o próprio art. 158-A, cadeia de custódia é "o conjunto de todos os procedimentos utilizados para manter e documentar a história cronológica do vestígio coletado em locais ou em vítimas de crimes, para rastrear sua posse e manuseio a partir de seu reconhecimento até o descarte" e é essencial para manter a integridade da prova para uma futura investigação criminal ou instrução processual penal.
[25] Art. 7º As informações do sistema de reconhecimento facial podem ser compartilhadas com órgãos de segurança pública de outros entes da Federação, especialmente com os integrantes operacionais do Sistema Único de Segurança Pública.
[26] Embora esta seja uma exigência para o compartilhamento internacional de dados, conforme art. 33, I da LGPD, trata-se de uma precaução significativa que o Distrito Federal pode adotar.
[27] Apesar de esta ser uma exigência do art. 7º, III da LGPD, que não necessariamente se aplica à segurança pública, o Distrito Federal contaria com mais salvaguardas se seguisse tal determinação, considerando a ausência de lei específica para a tecnologia ou sobre a proteção de dados na segurança pública em âmbito federal.
[28] § 1º O compartilhamento é possível no estrito limite desta Lei, sendo o destinatário das informações inteiramente responsável por sua utilização, exceto quando em operação conjunta com órgão do Distrito Federal.

anonimização ou o bloqueio destes, para que o destinatário repita o mesmo procedimento[29].

g. Do tempo de armazenamento dos dados

Por fim, o art. 7º, §2º da Lei Distrital estabelece um prazo máximo para a retenção dos dados obtidos por TRF, o que é relevante dentro do debate sobre a tecnologia. No entanto, **o prazo de 5 anos é excessivo**, especialmente se não está claro quais indivíduos terão seus dados armazenados: se de todos os rostos captados nas imagens ou apenas daqueles que, com a devida justificativa, foram objeto de análise do sistema.

Primeiramente, **os dados de pessoas não identificadas com os bancos de imagens de pessoas procuradas devem ser apagados imediatamente após a coleta**. E os dados que podem, em determinada situação, ser objetos de análise do sistema de reconhecimento facial devem receber tratamentos diferentes, de acordo com a motivação dessa análise.

A título de exemplo, uma pessoa, considerada desaparecida e que é posteriormente encontrada, pode ter seus dados eliminados em menos tempo que um indivíduo com um mandado de prisão em aberto. **É necessário que haja diferenciações** e, com base nestas, se estabeleça prazos distintos para a guarda.

Recomenda-se, ainda, que em qualquer das hipóteses, **o prazo não ultrapasse 6 meses**, extensíveis por mais 6 mediante autorização judicial caso já estejam sendo aplicados em investigações específicas, e que **revisões periódicas** sejam realizadas para atualização das informações[30].

[29] Essa é uma exigência do art. 17, §6º da LGPD, e se trata de um direito do titular dos dados, também em conformidade com o princípio geral da qualidade dos dados, presente no art. 6º, V.
[30] LGPD, arts. 15 e 16; Lynch, "Face Off: Law Enforcement Use of Face Recognition Technology".

IV - As matérias ausentes na Lei Distrital nº 6.712/2020

Ainda que o texto legal tenha se esgotado nos temas mencionados no capítulo anterior, há outras **matérias que não foram objeto da lei, mas que são de imensa relevância** para a implementação de TRF para segurança pública.

a. Da cibersegurança

A primeira questão se refere a medidas de segurança para proteção de dados - ou **cibersegurança**. A Lei Distrital nº 6.712/2020 não prevê qualquer diligência contra ciberataques ou acessos indevidos, o que contraria o princípio da segurança, previsto no art. 6º, VII da LGPD.

A segurança dos dados perpassa a tríade da **confiabilidade** - os dados são acessíveis apenas àqueles que possuem autorização de acesso; **integridade** - adota-se medidas de prevenção à manipulação e perda de dados; e **disponibilidade** - os dados estão à disposição quando requisitados[31].

Por se tratarem de dados biométricos, a obrigação é ainda mais imperativa, já que o acesso indevido à assinatura facial pode dar acesso também a outras informações pessoais a ela vinculadas[32]. Assim, para evitar situações indesejadas - ou até ilícitas - de destruição, perda, alteração, comunicação ou difusão de dados, é necessário que estes estejam protegidos por técnicas de **pseudonimização**. Dessa forma, os dados tornam-se ilegíveis para terceiros que não possuam a chave ou as informações

[31] European Data Protection Board, "Guidelines 3/2019 on processing of personal data through video devices", 29 de janeiro de 2020.
[32] Liu, *Bio-Privacy: Privacy Regulations and the Challenge of Biometrics*; Lynch, "Face Off: Law Enforcement Use of Face Recognition Technology".

adicionais necessárias para quebrar a pseudonimização. A técnica escolhida deve levar em consideração o contexto e ser adotada desde o desenho do sistema[33].

Além disso, como já mencionado anteriormente, deve haver restrição de acesso a profissionais autorizados e os dados, ainda que pseudonimizados, devem estar íntegros e disponíveis para acesso, tratamento e uso.

b. Do exercício de direitos pelo titular de dados

As medidas de cibersegurança, contudo, não podem obstar o **exercício de direitos pelo titular dos dados**. A LGPD especifica tais direitos em seu capítulo III e embora estes não possam ser absolutamente aplicáveis ao contexto de segurança pública, devem ser observados o mais fielmente possível. Destaca-se aqui os direitos ao acesso, correção, anonimização ou pseudonimização e eliminação de dados, bem como ao de informação sobre com quem seus dados foram compartilhados.

Na ausência de uma lei geral que estabeleça os limites para o exercício de tais direitos em face da necessidade de sigilo de investigações e processos penais, o Distrito Federal deve estabelecer um **procedimento para atender a solicitações** de acesso e modificação dos dados, prevendo inclusive a autoridade responsável por analisá-las e respondê-las e a possibilidade de recurso. Essa também é uma informação que deve ser divulgada pública e extensivamente[34].

Entretanto, o exercício dos direitos pelo titular não será plenamente possível se não houver transparência algorítmica e cuidados com a acurácia da tecnologia. A **transparência algorítmica** é um princípio que determina que qualquer decisão tomada por algoritmos deve ser inteligível e os critérios utilizados para tanto devem estar claros.

---

[33] Ricardo Bioni, *Proteção de dados pessoais: a função e os limites do consentimento*, 2019.

[34] Considerando a similaridade entre os regimentos de proteção de dados do Brasil e da União Europeia e a existência, neste sistema, de uma diretiva específica para segurança pública, o Distrito Federal pode buscar inspiração neste diploma legal. Para mais detalhes, ver: European Union, "Data Protection Law Enforcement Directive", Pub. L. No. (EU) 2016/680 (2016).

Para tanto, é necessário nitidez quanto aos dados utilizados para treinar o algoritmo (inputs) bem como à lógica do sistema, o que inclui informações a respeito de quais são os pesos dados pela aplicação às informações coletadas[35]. Além disso, vale discutir a respeito da possibilidade inclusive de tornar o código do sistema aberto, considerando que se trata de uma ferramenta utilizada para monitorar indivíduos acarretando em intrusões em sua liberdade. Conhecendo como e porquê o algoritmo atua, é possível contestar sua decisão - aspecto fundamental no âmbito da investigação e processo penal.

Quanto à **acurácia da tecnologia**, há diversos estudos que indicam a existência de vieses contra minorias em sistemas de reconhecimento facial, seja pelo treinamento inadequado dos algoritmos, seja pela baixa qualidade das imagens analisadas[36]. Logo, cuidados como testes anteriores da tecnologia contratada para garantia de alto percentual de acerto; adequação do perfil de similaridade de acordo com a finalidade

[35] Rader, Emilee, Kelley Cotter, and Janghee Cho. "Explanations as mechanisms for supporting algorithmic transparency." *Proceedings of the 2018 CHI conference on human factors in computing systems*. 2018.

[36] Tais estudos destacam a baixa performance dos sistemas ao analisar faces de pessoas de pele escura, mulheres e idosos. Para mais informações, conferir: Joy Buolamwini e Timnit Gebru, "Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification", *Proceedings of Machine Learning Research* 81 (2018): 1–15; Patrick Grother, Mei Ngan, e Kayee Hanaoka, "Face Recognition Vendor Test. Part 3: Demographic Effects" (Gaithersburg, MD: National Institute of Standards and Technology, dezembro de 2019), https://doi.org/10.6028/NIST.IR.8280; Inioluwa Deborah Raji e Joy Buolamwini, "Actionable Auditing: Investigating the Impact of Publicly Naming Biased Performance Results of Commercial AI Products", in *Proceedings of the 2019 AAAI/ACM Conference on AI, Ethics, and Society* (AIES '19: AAAI/ACM Conference on AI, Ethics, and Society, Honolulu HI USA: ACM, 2019), 429–35, https://doi.org/10.1145/3306618.3314244; Jacob Snow, "Amazon's Face Recognition Falsely Matched 28 Members of Congress With Mugshots", American Civil Liberties Union, 26 de julho de 2018,https://www.aclu.org/blog/privacy-technology/surveillance-technologies/amazons-face-recognition-falsely-matched-28.

de se obter o menor número de falsos positivos[37]; e priorização de sistemas que utilizem padrões técnicos reconhecidos por selos de qualidade[38].

Todas as informações relativas à acurácia da tecnologia e à transparência algorítmica devem estar disponíveis em relatórios técnicos e de acesso ao público e o sistema deve passar também por auditoria externa.

c. Da publicação de relatórios de impacto à proteção de dados e transparência

Ademais, antes do início das operações, é necessária a elaboração de um **relatório de impacto à proteção de dados**, nos termos do art. 5º, XVII da LGPD. Este documento deve conter "a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco" - ou seja, não apenas informações acerca de riscos cibernéticos, mas também uma análise jurídica.

Finalmente, após iniciada a implementação de TRF, recomenda-se a **publicação de relatórios periódicos para fins de transparência e controle social**. Isto porque apenas informações técnicas e pouco acessíveis não são suficientes para a aferição da regularidade e adequação dos sistemas de reconhecimento facial.

Tais relatórios devem conter informações como[39]:

---

[37] Sistemas de reconhecimento facial utilizam valores limiares para estabelecer o perfil de similaridade entre uma assinatura facial colhida de uma imagem e outra já presente na base de dados de pareamento. Valores mais altos podem levar a falsos negativos, situação em que assinaturas faciais contidas na base de dados não são reconhecidas quando comparadas a uma assinatura daquela mesma pessoa. Ao contrário, valores mais baixos levam a falsos positivos, quando uma pessoa é indevidamente reconhecida como sendo outra. Assim, considerando a sensibilidade dos dados e possibilidade de mal-entendidos com efeitos graves sobre a esfera íntima e social do indivíduo, é recomendável a adoção de valores mais altos. Para mais informações sobre perfil de similaridade, ver: Ian Berle, *Face Recognition Technology: Compulsory Visibility and Its Impact on Privacy and the Confidentiality of Personal Identifiable Images* (Springer Nature, 2020); K.W. Bowyer, "Face Recognition Technology: Security versus Privacy", *IEEE Technology and Society Magazine* 23, nº 1 (2004): 9–19, https://doi.org/10.1109/MTAS.2004.1273467; Lynch, "Face Off: Law Enforcement Use of Face Recognition Technology".

[38] Moraes, Almeida, e de Pereira, "Smile, You Are Being Identified! Risks and Measures for the Use of Facial Recognition in (Semi-)Public Spaces".

[39] Carolina Reis, "The Regulation of Data Privacy in Brazil: The Use of Facial Recognition Technology by Law Enforcement" (Master thesis, Germany, Universität Erfurt, 2020).

- quando, onde e por que a tecnologia foi utilizada;
- bases de dados utilizadas como fonte para pareamento;
- procedimentos adotados para abordagem policial a indivíduos identificados pela tecnologia como provavelmente compatíveis com pessoas procuradas;
- quantidade de dados coletados e armazenados;
- medidas adotadas para cibersegurança;
- indicadores de resultado, por exemplo, investigações criminais levadas a cabo com auxílio da tecnologia, inquéritos e processos penais baseados nos dados decorrentes de TRF, bem como crimes solucionados; e
- informações a respeito de compartilhamentos.

Ao seguir todas as recomendações, o Distrito Federal será capaz de implementar a Lei Distrital nº 6.712/2020 da forma mais adequada ao **respeito que o direito à proteção de dados exige**.

V - Resumo de recomendações para a Lei Distrital nº 6.712/2020

Este capítulo traz, de forma concisa, as recomendações contidas nas partes III e IV desta nota técnica. **Parte considerável dos aprimoramentos sugeridos podem ser implementados autonomamente pelo Distrito Federal**, seja por meio de modificações no texto da Lei nº 6.712/2020, seja de forma infralegal.

É importante salientar que, na ausência de lei geral de proteção de dados específica para o contexto da segurança pública, alguns pontos de atenção não podem ser objetos de normas legislativas pelo Distrito Federal. Ainda assim, **muitas dessas lacunas podem ser sanadas temporariamente** através de diretrizes e orientações para a implementação e uso de TRF em seu território.

Assim, as recomendações estão listadas abaixo e contêm uma breve explicação; a indicação do artigo da Lei Distrital a que o tema corresponde, caso haja; e a forma sugerida de determinação, se por vias legais ou infralegais.

Finalmente, aconselha-se que qualquer modificação deve **seguir os princípios e termos contidos na LGPD**, de maneira a uniformizar a linguagem e evitar discrepâncias.

1. Utilizar tecnologias de reconhecimento facial apenas em **casos excepcionais e determinados**, a fim de evitar a normalização e a vigilância em larga escala

Os **artigos 2º, II e 3º** definem vigilância contínua de forma ambígua, o que pode levar a interpretações e usos conflituosos com os direitos e garantias fundamentais. Utilizar tecnologias para vigilância irrestrita, ininterrupta e sem definição prévia de um alvo específico 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 seu consentimento.

Uma mudança no texto dos artigos só pode ocorrer por **alteração da Lei Distrital**. Contudo, sua **regulamentação via decreto** pode sanar eventuais divergências interpretativas, para **vedar, de forma explícita, a utilização de TRF** em desfavor de grupos de indivíduos indeterminados em qualquer contexto em que **não houver autorização judicial para tanto**.

2. Definir os **conceitos de espaços e equipamentos públicos** e restringir o uso da tecnologia em áreas próximas a organizações religiosas, políticas, de tratamento de saúde ou similares, de forma a evitar ao máximo a captura de dados de natureza sensível

O **art. 4º, caput** limita o uso da tecnologia a espaços e equipamentos públicos. Entretanto, tais conceitos não estão definidos no texto legal. É necessário **determiná-los** para evitar utilização em áreas indevidas ou exposição desnecessária de informações de indivíduos em situação de vulnerabilidade.

Além disso, a clareza das definições é capaz de **evitar a coleta de dados de cunho sensível,** como os de convicção religiosa, opinião política, filiação sindical ou a

organização de caráter religioso, filosófico ou político, ou, ainda, referente à saúde ou à vida sexual. Tais dados são irrelevantes para a prevenção e persecução penal e representam grave risco à proteção de dados.

Além disso, não utilizar TRF em protestos e manifestações, de modo a **evitar o *chilling effect***, situação em que indivíduos são desencorajados a exercer suas liberdades individuais por receio de perseguição penal e política.

A determinação de tais restrições espaciais pode ocorrer via **regulamentação por decreto**.

3. Estabelecer **protocolos de atuação e abordagem** a serem seguidos pelos agentes em caso de alertas emitidos pelo sistema e que possam ser consultados facilmente pela população

O **art. 5º, caput e parágrafo único**, institui a exigência de interferência humana em caso de alerta positivo emitido pelo sistema. Contudo, é necessário que tal atuação seja padronizada e adequada desde a emissão do alerta até a abordagem do indivíduo identificado. Além disso, é preciso **minimizar os riscos e danos causados por falsos positivos**, situações em que o sistema atribui a uma pessoa uma identidade que não corresponde àquela que ela realmente possui.

Estes protocolos, ainda que, para as autoridades, sejam distribuídos utilizando o jargão técnico policial, devem ser tornados públicos em linguagem simples e facilmente acessíveis pela população, e podem ser instituídos através de **diplomas infralegais**.

4. Definir **critérios para utilização da tecnologia**, tais como delimitar que seu uso seja feito exclusivamente em crimes de natureza grave, adotar mecanismos para minimizar o número de pessoas sujeitas a seu escrutínio e determinar o período máximo de aplicação, não ultrapassando 72h em nenhum caso

A Lei Distrital **não trata diretamente sobre tais questões**. Contudo, por se tratar de tecnologia com potencial tão invasivo, é preciso **limitar seu uso apenas ao estritamente necessário**. Assim, a TRF deve ser utilizada apenas quando não houver

outra maneira de se produzir a mesma prova. Tais limitações devem estar contidas em **decreto regulamentador**, ao menos enquanto não se edita lei federal a respeito.

Quanto a investigações e persecuções penais, provas obtidas por TRF só podem ser utilizadas quando o fato investigado constituir **infração penal de alto potencial ofensivo ou hediondo**. E, conforme a própria Lei Distrital, o uso da tecnologia para acompanhar as atividades do indivíduo, em tempo real ou em imagens previamente captadas, **não deve ultrapassar 72h**. Finalmente, deve-se produzir provas através de TRF apenas quando **houver indícios razoáveis da autoria ou participação em infração penal.** E determinados sujeitos devem ser excluídos do escrutínio da tecnologia em qualquer hipótese, como menores de idade.

5. Instituir **protocolos de controle de acesso aos dados** oriundos do sistema que restrinjam o tratamento de dados pessoais somente a pessoas que realmente necessitem acessar esses dados e registrem todos os acessos realizados

O **art. 6º** é pouco preciso ao determinar a restrição do tratamento de dados ao seu uso autorizado. Por isso, é necessário que haja limitação quanto à autorização de acesso, treinamento para o manejo do sistema e indicação e registro de data, hora e finalidade do login. Isso aumenta a **segurança dos dados** e faz parte da chamada **cadeia de custódia**, exigência do Código de Processo Penal.

Tais protocolos podem ser determinados via **diplomas infralegais**.

6. Identificar as **bases de dados utilizadas** como fonte para o pareamento de imagens analisadas pelo sistema e informá-las à sociedade

Esse é um **tema não tratado na Lei Distrital**. Toda assinatura facial captada pelo sistema será comparada a uma base de dados. Considerando que a TRF será utilizada para fins de segurança pública, é suficiente que as bases de dados sejam de **pessoas com mandado de prisão em aberto e desaparecidas**, assim como tem sido praxe em outros estados, como Rio de Janeiro e Bahia.

Outras bases de dados, como as de RGs e CNHs, contém informações irrelevantes para as atividades penais e podem levar ao desvirtuamento do uso da tecnologia, além

de ir contra o princípio da finalidade descrito na LGPD. É necessário, ainda, que tais bases de dados sejam **atualizadas constantemente** e **informadas à sociedade**.

Por inexistir texto legal que trate do tópico, a **regulamentação por decreto** pode instituir critérios mínimos de proteção de dados para as bases de dados escolhidas, ao passo que **diplomas infralegais** poderiam atualizar mais celeremente a lista de bases de dados que se adequam a tais critérios.

7. Estipular **categorias de dados pessoais**, definir **tempos de armazenamento** distintos de acordo com a sua natureza, não ultrapassando 6 meses em qualquer hipótese, e estabelecer **diretrizes para o compartilhamento** de dados

O **art. 7º, § 2º** estipula o prazo único para o armazenamento dos dados coletados por TRF. É preciso que haja **diferenciação** das categorias de dados de acordo com a **natureza do titular**. Assim, dados coletados via TRF de pessoas que não estiverem presentes em nenhuma das bases de dados de indivíduos que o Estado pretende identificar devem ser prontamente eliminados. Além disso, os dados armazenados devem ser revisados periodicamente para avaliar sua manutenção. Tal diferenciação pode ser instituída por meio de **regulamentação por decreto**.

Além disso, o **prazo máximo** de 5 anos é excessivo e deve ser reduzido. Tal período pode ser reduzido mediante **regulamentação** para o prazo sugerido de **6 meses**, extensíveis por mais 6 mediante autorização judicial caso já estejam sendo aplicados em investigações específicas.

Por fim, é necessário estabelecer **diretrizes para o compartilhamento de dados** oriundos de TRF com outros entes, conforme previsto no **art. 7º**, a fim de garantir a segurança dos dados e a transparência na operação.

Assim, as diretrizes devem estabelecer critérios para o compartilhamento, incluindo necessidade de **autorização específica para cada compartilhamento** através de regulamentação, convênio ou contrato entre as partes. O órgão receptor deve, ainda, certificar que assegura um grau de proteção adequado aos dados recebidos. **Diplomas infralegais** contendo tais diretrizes e instruções são suficientes.

8. Adotar **medidas de segurança e de proteção de dados**, inclusive pseudonimização

Esta é uma matéria **não tratada na Lei Distrital**, apesar de ser uma exigência da LGPD. Para evitar situações indesejadas - ou até ilícitas - de destruição, perda, alteração, comunicação ou difusão de dados, é necessário adotar técnicas de segurança e proteção dos dados, inclusive a pseudonimização. Dessa forma, os **dados tornam-se ilegíveis para terceiros**. A técnica escolhida deve levar em consideração o contexto e ser adotada desde o desenho do sistema.

De forma a sanar temporariamente a ausência, a matéria pode ser **regulamentada por decreto**, mas recomenda-se a inclusão de exigências de cibersegurança no próprio texto legal. Especificidades das medidas de segurança podem ser estabelecidas por **diplomas infralegais**.

9. Instaurar procedimentos para o **exercício de direitos do titular dos dados**

A Lei Distrital também **não tratou deste tema**, que também é uma exigência da LGPD. Por se tratar de um contexto distinto, a segurança pública requer **maior especificação de quais direitos o titular pode exercer**, como acesso, modificação e exclusão. Esses direitos podem ser **regulamentados via decreto**, observando sempre a LGPD.

Além disso, é necessário estabelecer **procedimentos para atender às solicitações** dos titulares de dados, prevendo inclusive a autoridade responsável por analisá-las e respondê-las e a possibilidade de recurso. Essa também é uma informação que deve ser divulgada pública e extensivamente. Os procedimentos podem ser instituídos via **diplomas infralegais**.

Além disso, é preciso instalar **placas informativas** nos locais onde a tecnologia será utilizada, acompanhadas de **documentos** físico e online que **contenham mais informações.**

Trata-se de determinação do **art. 4º, parágrafo único,** que só será efetiva se a placa contiver informações em **redação clara e acessível** e referência às identidades de controlador e encarregado, finalidades e base legal para o processamento dos dados e direitos do titular. A placa deve, ainda, estar em **local visível e em tamanho adequado**.

A placa deve estar acompanhada de **documentos online e físico** com informações mais detalhadas, instruções para o exercício dos direitos pelo titular e em linguagem compreensível. A determinação de tais diretrizes **via diplomas infralegais**, como portarias e instruções normativas, é suficiente para satisfazê-las.

10. Elaborar **relatório de impacto à proteção de dados (RIPD)** antes da implementação da tecnologia e divulgar **relatórios de transparência**, de forma periódica, que contenham informações acerca do uso e dos resultados da tecnologia

A Lei Distrital **não traz qualquer previsão** a respeito da elaboração de RIPD, apesar de também ser uma **obrigação contida na LGPD**. Como a própria LGPD explica, RIPD é "a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco".

Portanto, deve conter não apenas informações acerca de **riscos cibernéticos**, mas também uma **análise jurídica** sobre o uso. Especial atenção deve se dar à transparência algorítmica e à precisão da tecnologia.

A **regulamentação por decreto** é capaz de determinar a exigência de elaboração de RIPD, ao passo que **diplomas infralegais** podem instituir os critérios de conteúdo e forma do relatório.

Por fim, a Lei Distrital também **não trata sobre a matéria** da transparência e prestação de contas. Por ser uma tecnologia tão invasiva, é necessário que a sociedade e organizações sociais sejam capazes de **averiguar a regularidade e adequação** dos sistemas de reconhecimento facial. **Relatórios periódicos e em linguagem acessível** são uma ferramenta para isso.

Tais relatórios devem conter informações como:

- quando, onde e por que a tecnologia foi utilizada;
- bases de dados utilizadas como fonte para pareamento;
- quantidade de dados coletados e armazenados;
- medidas adotadas para cibersegurança;

- indicadores de resultado que incluam, por exemplo, investigações criminais levadas a cabo com auxílio da tecnologia, inquéritos e processos penais baseados nos dados decorrentes de TRF, bem como crimes solucionados; e
- informações a respeito de compartilhamentos.

O **decreto regulamentador** também deve incluir a exigência de mecanismos de controle social, enquanto **diplomas infralegais** devem determinar sua forma e conteúdo.

VI - Conclusão

A Lei Distrital nº 6.712/2020 **traz alguns pontos positivos** para a regulação da aplicação de reconhecimento facial, **ao passo que traz dispositivos preocupantes** - seja por insuficiência de sua redação, seja por total ausência de previsão a respeito.

A presente Nota Técnica, portanto, objetivou a discussão do conteúdo da Lei Distrital, ao passo que propôs medidas para adequar seu texto às exigências do direito fundamental à proteção de dados. Tais medidas podem ser acolhidas, em alguns casos, através da mudança da própria Lei Distrital nº 6.712/2020 e também por meio de diplomas infralegais.

Assim, o LAPIN sugere a **análise dos pontos apresentados nos termos descritos neste documento e a adoção das recomendações propostas**, de modo a garantir uma regulamentação do uso de TRF para segurança pública no Distrito Federal pertinente aos parâmetros previstos pelo sistema de proteção de dados brasileiros e internacionais.

Anexo: tabela com recomendações

Recomendação	Artigos da Lei	Justificativa breve	Forma sugerida de determinação
Utilizar TRF apenas em situações excepcionais	2, II e 3 *caput*	Evita-se a normalização e a vigilância em larga escala	Alteração da Lei; Regulamentação por decreto
Estipular categorias de dados e definir tempos de armazenamento distintos, não ultrapassando 6 meses	7 *caput* e § 2º	Amplia-se a segurança dos dados e condiz com as exigências da LGPD	
Definir os conceitos de espaço e equipamento públicos	4	Evita-se o *chilling effect*, bem como a captura de dados de cunho íntimo	Regulamentação por decreto
Restringir o uso de TRF em determinados espaços, ainda que públicos			
Definir condições para a utilização da tecnologia quanto aos tipos penais, duração máxima e pessoas sujeitas	*	Reduz-se a margem para desvirtuamento do uso da tecnologia	
Instalar placas informativas adequadas, acompanhadas de documentos físico e online	4, parágrafo único	Condiz com as exigências da LGPD e aumenta a transparência no uso	Regulamentação por decreto; Determinação de diretrizes via diplomas infralegais
Determinar as bases de dados fonte do pareamento	*	Reduzem-se os riscos de vigilância em larga escala e aumenta a transparência	
Adotar medidas de segurança e proteção de dados, inclusive pseudonimização	*	Amplia-se a segurança dos dados	
Instituir procedimentos para o exercício de direitos pelo titular dos dados	*	Condiz com as exigências da LGPD	
Elaborar relatórios periódicos para publicização	*	Condiz com as exigências da LGPD e aumenta a transparência	

Estabelecer protocolos de atuação e abordagem em caso de alerta	5 *caput* e parágrafo único	Minimiza-se os riscos e danos causados por falsos positivos	Determinação de diretrizes via diplomas infralegais
Instituir protocolos de autorização restrita para acesso aos dados	6 *caput*	Amplia-se a segurança dos dados e condiz com as exigências do Código de Processo Penal	
Estabelecer diretrizes para o compartilhamento de dados	7 *caput* e § 1º	Amplia-se a segurança dos dados e aumenta a transparência	
Realizar RIPD antes de qualquer implementação	*	Condiz com as exigências da LGPD e aumenta a transparência	
*** Trata-se de recomendação não-vinculada a qualquer artigo da lei**			