XIII ENCONTRO INTERNACIONAL DO CONPEDI URUGUAI – MONTEVIDÉU

GOVERNO DIGITAL, DIREITO E NOVAS TECNOLOGIAS I

DANIELLE JACON AYRES PINTO

YURI NATHAN DA COSTA LANNES

LAURA INÉS NAHABETIÁN BRUNET

Copyright © 2024 Conselho Nacional de Pesquisa e Pós-Graduação em Direito

Todos os direitos reservados e protegidos. Nenhuma parte destes anais poderá ser reproduzida ou transmitida sejam quais forem os meios empregados sem prévia autorização dos editores.

Diretoria – CONPEDI
Presidente - Profa. Dra. Samyra Haydêe Dal Farra Naspolini - FMU – São Paulo
Diretor Executivo - Prof. Dr. Orides Mezzaroba - UFSC – Santa Catarina
Vice-presidente Norte - Prof. Dr. Jean Carlos Dias - Cesupa – Pará
Vice-presidente Centro-Oeste - Prof. Dr. José Querino Tavares Neto - UFG – Goiás
Vice-presidente Sul - Prof. Dr. Leonel Severo Rocha - Unisinos – Rio Grande do Sul
Vice-presidente Sudeste - Profa. Dra. Rosângela Lunardelli Cavallazzi - UFRJ/PUCRio – Rio de Janeiro
Vice-presidente Nordeste - Prof. Dr. Raymundo Juliano Feitosa - UNICAP - Pernambuco

Representante Discente: Prof. Dr. Abner da Silva Jaques - UPM/UNIGRAN - Mato Grosso do Sul

Conselho Fiscal:
Prof. Dr. José Filomeno de Moraes Filho - UFMA - Maranhão
Prof. Dr. Caio Augusto Souza Lara - SKEMA/ESDHC/UFMG - Minas Gerais
Prof. Dr. Valter Moura do Carmo - UFERSA - Rio Grande do Norte
Prof. Dr. Fernando Passos – UNIARA - São Paulo
Prof. Dr. Edinilson Donisete Machado - UNIVEM/UENP - São Paulo
Secretarias
Relações Institucionais:
Prof. Dra. Claudia Maria Barbosa - PUCPR - Paraná
Prof. Dr. Heron José de Santana Gordilho - UFBA - Bahia
Profa. Dra. Daniela Marques de Moraes - UNB - Distrito Federal
Comunicação:
Prof. Dr. Robison Tramontina - UNOESC - Santa Catarina
Prof. Dr. Liton Lanes Pilau Sobrinho - UPF/Univali - Rio Grande do Sul
Prof. Dr. Lucas Gonçalves da Silva - UFS - Sergipe
Relações Internacionais para o Continente Americano:
Prof. Dr. Jerônimo Siqueira Tybusch - UFSM - Rio Grande do Sul
Prof. Dr. Paulo Roberto Barbosa Ramos - UFMA - Maranhão
Prof. Dr. Felipe Chiarello de Souza Pinto - UPM – São Paulo
Relações Internacionais para os demais Continentes:
Profa. Dra. Gina Vidal Marcilio Pompeu - UNIFOR - Ceará
Profa. Dra. Sandra Regina Martini - UNIRITTER / UFRGS - Rio Grande do Sul
Profa. Dra. Maria Claudia da Silva Antunes de Souza - UNIVALI – Santa Catarina
Eventos:
Prof. Dr. Yuri Nathan da Costa Lannes - FDF - São Paulo
Profa. Dra. Norma Sueli Padilha - UFSC - Santa Catarina
Prof. Dr. Juraci Mourão Lopes Filho - UNICHRISTUS - Ceará

Membro Nato – Presidência anterior Prof. Dr. Raymundo Juliano Feitosa – UNICAP – Pernambuco

D597

GOVERNO DIGITAL, DIREITO E NOVAS TECNOLOGIAS I

[Recurso eletrônico on-line] organização CONPEDI

Coordenadores: Danielle Jacon Ayres Pinto, Yuri Nathan da Costa Lannes, Laura Inés Nahabetián Brunet – Florianópolis: CONPEDI, 2024.

Inclui bibliografia
ISBN: 978-85-5505-986-5
Modo de acesso: www.conpedi.org.br em publicações
Tema: ESTADO DE DERECHO, INVESTIGACIÓN JURÍDICA E INNOVACIÓN

1. Direito – Estudo e ensino (Pós-graduação) – 2. Governo digital. 3. Novas tecnologias. XIII ENCONTRO INTERNACIONAL DO CONPEDI URUGUAI – MONTEVIDÉU (2: 2024 : Florianópolis, Brasil).

CDU: 34



Conselho Nacional de Pesquisa
e Pós-Graduação em Direito Florianópolis
Santa Catarina – Brasil
www.conpedi.org.br

XIII ENCONTRO INTERNACIONAL DO CONPEDI URUGUAI – MONTEVIDÉU

GOVERNO DIGITAL, DIREITO E NOVAS TECNOLOGIAS I

Apresentação

O XIII ENCONTRO INTERNACIONAL DO CONPEDI URUGUAI – MONTEVIDÉU, realizado na Universidad de La República Uruguay, entre os dias 18 a 20 de setembro de 2024, apresentou como temática central "Estado de Derecho, Investigación Jurídica e Innovación". Esta questão suscitou intensos debates desde o início e, no decorrer do evento, com a apresentação dos trabalhos previamente selecionados, fóruns e painéis que ocorreram na cidade de Montevidéu-Uruguai.

Os trabalhos contidos nesta publicação foram apresentados como artigos no Grupo de Trabalho "DIREITO, GOVERNANÇA E NOVAS TECNOLOGIAS I", realizado no dia 20 de setembro de 2024, que passaram previamente por no mínimo dupla avaliação cega por pares. Encontram-se os resultados de pesquisas desenvolvidas em diversos Programas de Pós-Graduação em Direito, que retratam parcela relevante dos estudos que têm sido produzidos na temática central do Grupo de Trabalho.

As temáticas abordadas decorrem de intensas e numerosas discussões que acontecem pelo Brasil, com temas que reforçam a diversidade cultural brasileira e as preocupações que abrangem problemas relevantes e interessantes, a exemplo do direito digital, proteção da privacidade, crise da verdade, regulamentação de tecnologias, transformação digital e Inteligência artificial, bem como políticas públicas e tecnologia.

Espera-se, então, que o leitor possa vivenciar parcela destas discussões por meio da leitura dos textos. Agradecemos a todos os pesquisadores, colaboradores e pessoas envolvidas nos debates e organização do evento pela sua inestimável contribuição e desejamos uma proveitosa leitura!

Danielle Jacon Ayres Pinto - Universidade Federal de Santa Catarina

Yuri Nathan da Costa Lannes - Faculdade de Direito de Franca

Laura Inés Nahabetián Brunet - Universidad Mayor de la República Oriental del Uruguay

RECONHECIMENTO FACIAL NA SEGURANÇA PÚBLICA: RISCOS, REGULAMENTAÇÕES E CONSIDERAÇÕES ÉTICAS

FACIAL RECOGNITION IN PUBLIC SECURITY: RISKS, REGULATIONS, AND ETHICAL CONSIDERATIONS

Lais Faleiros Furuya
Yuri Nathan da Costa Lannes
Larissa Maia Freitas Salerno Miguel Santos

Resumo

O artigo científico discute o uso do reconhecimento facial na segurança pública, focando especialmente no Estado de São Paulo. A pesquisa aborda os riscos e preocupações associados a essa tecnologia, destacando questões de privacidade, proteção de dados, erros de identificação e discriminação racial. Utilizando uma abordagem metodológica qualitativa com revisão bibliográfica e análise documental, o estudo investiga a implementação de câmeras corporais com reconhecimento facial por policiais militares, analisando aspectos técnicos, legais e sociais. Os objetivos incluem examinar a legislação vigente, avaliar os impactos éticos e sociais, identificar erros e discriminação, e propor diretrizes para regulamentação eficaz e ética da tecnologia. Conclui-se que, embora o reconhecimento facial ofereça benefícios em segurança, há riscos significativos que requerem regulamentação específica, transparência na operação e treinamento adequado dos operadores para mitigar tais problemas. Recomenda-se que legisladores e gestores públicos considerem essas conclusões para garantir um uso responsável e justo do reconhecimento facial, equilibrando segurança pública com proteção dos direitos individuais.

Palavras-chave: Reconhecimento facial, Segurança pública, Proteção de dados, Regulação, Câmeras corporais da polícia

Abstract/Resumen/Résumé

The scientific article discusses the use of facial recognition in public security, focusing particularly on the state of São Paulo, Brazil. The research addresses the risks and concerns associated with this technology, highlighting issues of privacy, data protection, identification errors, and racial discrimination. Using a qualitative methodological approach with literature review and document analysis, the study investigates the implementation of body-worn cameras with facial recognition by military police, analyzing technical, legal, and social aspects. Objectives include examining current legislation, assessing ethical and social impacts, identifying errors and discrimination, and proposing guidelines for effective and ethical regulation of the technology. It concludes that while facial recognition offers security benefits, there are significant risks that require specific regulation, operational transparency,

and adequate training of operators to mitigate these issues. It is recommended that lawmakers and public officials consider these findings to ensure responsible and fair use of facial recognition, balancing public security with protection of individual rights.

Keywords/Palabras-claves/Mots-clés: Facial recognition, Public security, Data protection, Regulation, Police body-worn cameras

1 INTRODUÇÃO

O presente artigo científico abordará o tema relacionado ao uso do reconhecimento fácil. Esta temática tem se tornado uma ferramenta amplamente discutida no contexto da segurança pública e especialmente no Brasil tem levantado algumas preocupações. A tecnologia permite a identificação de indivíduos por meio de características faciais e tem sido implementada em diversas áreas na segurança pública, desde o controle de fronteiras até o monitoramento de eventos públicos. A pesquisa abordará os possíveis riscos e violações associadas ao uso do reconhecimento facial, com foco na segurança pública do Estado de São Paulo, visando compreender os desafios e implementações legais destas práticas.

Esse estudo se concentra na análise do uso de câmeras corporais com reconhecimento fácil vestidas por policiais militares do Estado de São Paulo. A pesquisa se delimita a explorar os aspectos técnicos, legais e sociais desta tecnologia, considerando a implementação recente e os requisitos exigidos pela Diretoria de Tecnologia da Informação e Comunicação (DTIC), do Governo do Estado de São Paulo. A análise também abrange a regulamentação vigente e a necessidade de maior transparência e controle no uso destas ferramentas.

A problemática central desta pesquisa concentra-se na investigação dos riscos e violações decorrentes do uso de reconhecimento facial em câmeras operadas por policiais militares. Entre as questões problemáticas estão a potencial violação de direitos fundamentais, como a privacidade e a proteção de dados pessoais, além de possíveis erros de identificação e discriminação racial. A pesquisa busca esclarecer como esses problemas podem ser mitigados e quais são as medidas necessárias para assegurar o uso ético e eficiente dessa tecnologia. Assim, a pergunta que a pesquisa pretende responder é: quais os riscos relacionados a tecnologia de reconhecimento fácil em câmeras utilizadas pela segurança pública e de quais maneiras se poderia mitigar tais riscos?

Entre as hipóteses a serem verificadas podemos elencar que: a utilização de reconhecimento facial em câmeras operadas por policiais militares pode resultar em violação de direitos fundamentais como a privacidade e a proteção de dados; a falta de regulamentação específica e transparência no uso dessas tecnologias aumenta os riscos de erros de identificação e discriminação contra populações já vulneráveis e; a implementação adequada de normas legais e procedimentos técnicos podem mitigar os riscos associados ao reconhecimento facial na segurança pública.

Objetiva-se com o estudo analisar os riscos e violações associados ao uso de câmeras com reconhecimento facial por policiais militares no Estado de São Paulo, propondo recomendações para uma regulamentação eficaz e ética dessa tecnologia. Entre os objetivos específicos se pode propor: o exame da legislação vigente sobre o uso de reconhecimento fácil e sua aplicação na segurança pública; avaliação; avaliação dos impactos sociais e éticos da utilização de reconhecimento facial em câmeras; identificação de casos de erros de identificação e discriminação relacionados ao uso desta tecnologia e; apresentar possíveis diretrizes e recomendações para a regulamentação do uso de reconhecimento fácil na segurança pública.

A pesquisa se justifica pela crescente implementação de tecnologias de reconhecimento facial no Brasil e os riscos associados a sua utilização indiscriminada. A ausência de regulamentação específica e a falta de transparência no uso destas tecnologias podem levar a sérias violações de direitos humanos, além de discriminação racial. Este estudo pretende, assim, contribuir para o debate sobre o tema de normas claras e eficientes, garantindo que o uso do reconhecimento fácil seja seguro, ético e respeite os direitos dos indivíduos.

A pesquisa adota uma abordagem metodológica qualitativa, utilizando de revisão bibliográfica e análise de documentos e estudos que verifiquem a arquitetura de tecnologias de reconhecimento facial. Para tanto, serão analisados relatórios técnicos, legislação e artigos científicos e casos práticos relacionados ao uso de reconhecimento facial na segurança pública. Além disso, serão analisados casos específicos, como o uso de câmeras no carnaval de 2019 no Rio de Janeiro, com a finalidade de ilustrar os problemas e desafios identificados.

O trabalho está estruturado em capítulos que abordarão o tema na seguinte ordem: a exposição dos riscos existentes ao manusear uma ferramenta de reconhecimento facial, especialmente quando utilizada para fins de política pública, em seguida um destrinchamento às possíveis regulações legais e extramuros em termos legislativos e por fim a análise do edital nº nº15/2024 com o objeto da implementação de câmeras corporais com emprego de IA para fins de identificação de pessoas e coisas.

2.1 RISCOS E VIOLAÇÕES DO USO DO RECONHECIMENTO FACIAL

Considerado a finalidade em aprimorar ferramentas na segurança pública, especialmente no âmbito do uso da Inteligência Artificial, haverá inicialmente neste capítulo o desdobramento dos riscos oferecidos pelo uso do reconhecimento facial, especialmente com auxílio de dados abordados pelo Laboratório de Políticas Públicas e Internet (Lapin, 2021), cujo

objetivo ecoa-se em conduzir estudos sobre a respectiva ferramenta e os impactos na segurança pública e na sociedade como um todo.

Não se trata de uma afirmação surpresa quando enfatiza o uso do reconhecimento facial em sistemas de vigilância para fins de segurança pública. É cristalino também que o respectivo uso foi possível pela ascensão da Inteligência Artificial cumulada à big data, ou popularmente conhecido como base de dados (Costa, Negri e Oliveira, 2020, p. 4).

No Brasil a implementação desta ferramenta de Inteligência Artificial ocorreu em 2011, na cidade de Ilhéus localizada no Estado da Bahia. Contudo a sua popularização se deu mesmo em 2019 sucedendo-se ao cenário atual em que o reconhecimento facial se revela em ramos públicos como na educação, transporte, controle de fronteiras e segurança pública, cujo este último será o enfoque desta pesquisa (Instituto Igarapé, 2019).

Uma das formas possíveis de explicar o uso massivo do referido equipamento artificial compreende o universo das cidades inteligentes. Dentro desta órbita, há a alta capacidade no cruzamento de dados e informações dos quais facilita o cuidado Estatal frente ao progresso da população de um determinado Estado. Deste modo, tecnologias artificiais como o reconhecimento facial unidos à gestão do Estado foram uma saída lógica para uma gestão estatal funcional em face do crescimento populacional (Costa, Negri e Oliveira, 2020, p. 4).

De uma forma genérica, segundo Costa, Negri e Oliveira, o reconhecimento facial na segurança pública tem sua funcionalização resumida em quatro fases. Inicialmente o rosto de um determinado cidadão é identificado para que posteriormente o sistema de software possa estabelecer uma "assinatura facial" (2020, p. 6), reconhecendo por sua vez as medidas existentes entre os olhos e entre a parte superior e inferior do rosto. Após essa análise técnica, o processo de acareação inicia-se, colocando lado a lado, os rostos pertencentes ao banco de dados compostos por foragidos, e o rosto capturado inicialmente. Por fim, findando todo esse processo, torna-se possível atribuir a real identidade do cidadão reconhecido.

Acontece que apesar de aparecer um procedimento simples, há variantes prejudiciais para o cidadão que está sendo reconhecido. O primeiro cenário compreende pelo risco existente no tipo de dados utilizado, isto é, dados sensíveis, dos quais uma vez identificado estes já fazendo parte de um universo de informações não havendo possibilidade de uma possível anuência em ser ou não reconhecido novamente (Lapin, 2021, p. 5), e logicamente não há autorização do titular no momento do reconhecimento.

Um segundo ponto é o da discriminação, ora reconhecer erroneamente ora ser impossível o reconhecimento. Um cenário que enfatizou esse risco foi no contexto do Carnaval de 2019 no Rio de Janeiro em que um homem foi preso por engano em decorrência do equívoco

do reconhecimento facial formado um por uma big data repleta de mandados de prisão a serem cumpridos (Lapin, 2021, p. 51). Este episódio enquadra-se exatamente no primeiro risco abordado pela análise realizada pelo Laboratório de Políticas Públicas e Internet (LAPIN), isto é, na violação de Direitos Fundamentais (2020, p.8). O caso comentado enfatiza duas pessoas inocentes em que a princípio foram abordadas como suspeitas além de sofrerem o constrangimento de serem encaminhadas à delegacia para só após a devida averiguação serem liberadas.

Se houve um tratamento em que a presunção de inocência foi violada, logo a honra e a imagem destas pessoas que foram reconhecidas de maneira equivocada também foram violadas e, por conclusão, o direito à proteção dos dados sensíveis também foram afetados (Lapin, 2021, p.8).

Acontece que a partir do momento que o indivíduo está sendo monitorado sem sua autorização, resta claro a tecnologia abordada pelo poder Estatal passa a andar na contramão ao do artigo 2º, inciso I e IV da Lei Geral de Proteção de Dados Pessoais (Brasil, 2018). A lesão à privacidade, intimidade, honra e à imagem é o que se ataca quando há uma vigilância pelo reconhecimento facial para fins de segurança pública realizada de maneira equivocada. Convém indicar ao pesquisador que esses direitos não foram inéditos na LGPD, constando muito antes na Carta Magna de 1988, compreendendo apenas um empréstimo de termos à Lei Geral de Proteção de Dados (Fachin, Leite, 2023, p.10)

A ferramenta de reconhecimento facial para ter seu perfeito funcionamento precisa de um banco de dados. Há uma função matemática entre essa ferramenta de vigilância com a inteligência artificial e os dados nela inseridos e este cenário obviamente gera abalos nas informações e aos seus titulares, especialmente quando esses dados não são cuidados e utilizados com exatidão (Costa, Kremer, 2022, p. 2).

Dentro deste mesmo raciocínio, mas seguindo uma vertente diferente, está o racismo e a falta de precisão na identificação. A presença de modelos matemáticos algoritmos são definidos mediante um padrão cujo seu criador está inserido, isentando de qualquer critério racial. Por consequência, os dados inseridos são aqueles responsáveis por treinar esses algoritmos, e a partir do momento que estas informações não são diversificadas, logo os algorítmicos também não serão (Coimbra, Moraes, Silva, 2023, p. 17).

Estes mesmos pesquisadores (2023, p. 15 – 4) detalham a respeito de um programa utilizado pelo Poder Judiciário do Estados Unidos, denominado de *Correctional Offender Management Profiling For Alternative Sanctions*, com o intuído de identificar quais as chances do executado ser reincidente. Os parâmetros utilizados foram “local de residência, histórico de

envolvimento com drogas, antecedentes familiares e desempenho escolar" (2023, p. 15), tendo por resultado que as maiores chances seriam para as pessoas negras.

Absurdamente seria afirmar que o reconhecimento facial programado com eles algorítmicos o qual é utilizado para fins de segurança pública, lhe ocasiona um reconhecimento de repressão para uma pessoa negra que ao final de uma possível averiguação seria apenas uma vítima do engano. O dilema está na compreensão daquele que irá elaborar o algoritmo do reconhecimento facial em relação ao que o Estado quer vigiar e conter em prol da segurança do cidadão no geral (Costa, Kremer, 2022, p. 2).

Não somente, mas quanto à precisão, o pesquisador Pablo Nunes (2019, p. 69) destaca um ponto crucial, em que a assinatura digital é configurada por medidas localizadas e não por completo, gerando a falta de precisão. Não somente, mas de acordo com o pesquisador (2019, p. 69) a exatidão há de ter inclusive nas medidas de semelhança ao passo que o nível similitude menor que 90% ocasionaram falsos positivos, mas um nível em 99,9% seria muito preciso a ponto de quase não conseguir haver o reconhecimento com o banco de dados. Para exemplificar, Nunes relata o Carnaval de 2019 em Feira de Santana, município da Bahia, em que houve 903 avisos pelo reconhecimento, mas apenas 33 casos foram levados adiante, ou seja, 4% dos avisos foram de fato significativos (2019, p. 70).

Um outro ponto para se tratar como uma variante é possível risco no reconhecimento facial é a finalidade e a transparência destes mesmos dados biométricos que serão captados no momento que a assinatura facial é determinada (Lapin, 2021, p.8). Em termos legais a LGPD, em seu extenso artigo 6º, enumera exaustivamente princípios pelos quais o tratamento de dados pessoais deve percorrer, descrevendo, respectivamente, a finalidade e a transparência como a forma de tratar essas informações e a possibilidade de justificar do porquê os dados biométricos estão sendo captados (Brasil, 2018).

O que acontece é que apesar destas claras diretrizes, quando a ferramenta artificial é operacionalizada em grandes proporções como em um episódio carnavalesco, o princípio da finalidade e da transparência é dificilmente respeitado. Um estudo realizado em 2021 pelo mesmo Laboratório de Políticas Públicas e Internet (2021, p. 11) indicou que o uso de reconhecimento facial pelo Polícia Civil do Estado de São Paulo não havia legislação para fins regulatórios, e inclusive não havia informações suficientes para identificar possíveis erros e acertos e boas práticas pelo uso da ferramenta.

Além de enumerar esses exaustivos riscos na ferramenta de vigilância pública, a LAPIN (2021, p. 13) enumera cinco principais variantes no reconhecimento facial, sejam elas: a regulação, os meios de aquisição, o conhecimento técnico de responsáveis pela

implementação do reconhecimento facial, o impacto dessas tecnologias e a prestação de contas no seu uso.

A partir de um destrinchamento destes cinco pontos, a primeira conclusão deste relatório é a insuficiência de legislações específicas e reguladoras nestas ferramentas de vigilância. Não somente, mas o termo discricionariedade é o que se aparece de forma negativa no relatório de maneira que quando a ferramenta apresenta instabilidades, a discricionariedade não é muito bem-vista (Lapin, 2021, p. 19).

Nesta mesma linha, une-se ao afirmando anteriormente quanto à instabilidade de princípios da proteção de dados pessoais no que se refere ao reconhecimento facial, sejam eles ao da finalidade, da transparência, da não discriminação. O que ocorre é que no artigo 26º da LGPD, há uma diretriz determinando que o Poder Público deve fazer uso dos dados pessoais respeitando os referidos princípios (Brasil, 2018). Contudo, com um simples raciocínio, conclui-se que o gestor tem em mãos apenas uma discricionariedade é uma ferramenta de vigilância que corre em linha contrária ao artigo supramencionado, sendo muito bem exemplificado no Carnaval de 2019 no Rio de Janeiro (Lapin, 2021, p. 15).

Já a segunda conclusão deste relatório é a influência na origem no uso de tecnologias de vigilância, que também é eixo e objeto desta pesquisa, cujo resultado do respectivo relatório identifica três pontos; primeiro a sua pequena concorrência, segundo a origem dos sistemas de países da China, Israel, Estados Unidos e Reino Unido e pôr fim a aquisição oriunda meios licitatórios e diversas formas de acordos (Lapin, 2021, p. 22). Para fins exploratórios, na cidade de Campinas em 2018 a empresa chinesa Huawei disponibilizou 30 (trinta) câmeras de monitoramento inseridos no projeto chamado “Cidade Segura” com parceria do Centro de Pesquisa e Desenvolvimento em Telecomunicações e com a prefeitura de Campinas (Instituto Igarapé, 2019). Estes equipamentos foram integrados na Central Integrada de Monitoramento de Campinas com o fim de segurança pública, não muito diferente das câmeras fornecidas pela Hikvision na cidade de São Paulo, o qual é também de origem chinesa (Lapin, 2021, p. 23).

Mostra-se diante deste relatório que há um fornecimento estrangeiro de equipamentos que vem a ser usado no ambiente brasileiro, no qual ora os preços são consideravelmente mais chamativos em relação às empresas nacionais, ora havia “acordos de cooperação” em que empresas particulares detinham interesses comuns com a administração pública (2021, p. 23).

Entretanto, o assunto torna-se ainda mais preocupante quando se verifica que segundo as pesquisas extraídas pela Privacy.co, equipamentos de vigilância das marcas Hikvision e Dahua são protagonistas em infringir garantias básicas em função da sua capacidade em

estereotipar os indivíduos reconhecidos especialmente com um caráter racial (Costa, Kremer, 2022, p. 2).

O ponto que se pretende chegar a partir desta explanação é que apesar da utilização de equipamentos com origens estrangeiras é essencial que o tratamento dos dados devem ser transparentes nos termos da LGPD, do artigo 23, inciso I e mais que isso, que a execução de atividades que fazer o uso destes mesmos dados seja realizada dentro da previsão legal (Brasil, 2018). Para findar este raciocínio, convém declinar que este mesmo discurso legal não é apenas da Lei Geral de Proteção de Dados, mas também do Marco Civil da Internet no rol exaustivo do artigo 24, especialmente que condiz no desenvolvimento da internet pelo poder público de maneira transparente, colaborativa e democrática (Brasil, 2014).

Partindo para uma outra ótica, mais especificamente para a terceira variante, está a percepção da tecnologia artificial de reconhecimento daquele que o manuseia. Talvez seja até possível afirmar a existência de um efeito cascata de maneira que a inexistência de uma legislação específica e cautelosamente elaborada gera dedutivamente a inexistência da determinação em delegar o conhecimento sobre a respectiva ferramenta da empresa ao operador.

Mais uma vez a afirmação acompanha-se de um caso fático, isto é, o mesmo projeto "Cidade Segura" da cidade de Campinas que apesar de designar o uso da ferramenta de vigilância, não certificou sobre a importância de conferir o manuseio da ferramenta e o conhecimento nela inserido. Kremer e Costa (2022, p. 17) expõem adequadamente que "a transparência sobre a criação e funcionamento dessas tecnologias também é princípio basilar para o uso de tecnologias". Ora é visível que para o reconhecimento facial utilizado para fins de segurança pública é necessário um conhecimento técnico, especialmente em face dos potenciais riscos aqui já expostos e exemplificados, especialmente os falsos positivos e os falsos negativos (Lapin, 2021, p. 49).

Caminhando para o final, na quarta variável é possível mais uma vez indicar os termos legais na LGPD, precisamente na obrigatoriedade dos chamados relatórios de impacto à proteção de dados pessoais. No cerne da segurança pública, os operadores de dados pessoais estão sujeitos a realizar o respectivo documento. Segundo os dados do projeto de pesquisa O Panóptico: Monitor do Reconhecimento Facial no Brasil, coordenado por Pablo Nunes (Nunes, 2020), há 16.287.222 (dezesseis milhões, duzentos e oitenta e sete mil, duzentos e vinte e duas) pessoas monitoradas pelo reconhecimento facial no Estado de São Paulo. Paralelamente, nos termos do relatório realizado pelo Laboratório de Políticas Públicas e Internet, foram realizados vinte e cinco pedidos mediante a Lei de Acesso à Informação. O resultado foi que além do

desconhecimento pelo relatório a ser realizado, não houve retorno pela Administração Pública sobre a identificação documental dos impactos sobre os dados pessoais destas pessoas monitoradas (Lapin, 2021, p. 30).

Para essa simples pesquisa, mostra-se sem esforço o número de pessoas submetidas à tecnologia artificiais, mas sequer controle pela operadora do reconhecimento facial sobre os riscos pelo qual os dados biométricos são submetidos.

Por fim e não menos importante, a prestação de contas reflete também um efeito cascata ao passo que o efeito negativo referente ao não fornecimento do relatório de impacto à proteção de dados pessoais implica na abstenção em prestar contas sobre como esses dados biométricos são tratados e para que eles são captados (Lapin, 2021, p. 37).

A problemática está que a prestação do serviço público justificaria o uso legítimo de dados pessoais, porém conforme demonstrado a Administração Pública não indica informações de como esses dados são tratados. Ora, o assunto central compreende em uma ferramenta que cuida de dados pessoais, contudo durante a pesquisa realizada pela LAPIN em 2021 (2021, p. 48), houve dois pedidos de informações, ambos fundada pela Lei de Acesso à Informação, para a Polícia Civil do Estado de São Paulo, tendo como retorno uma resposta negativa.

Diante desse cenário dramático, a primeira consequência configura-se no erro de falso positivo ocorrido no reconhecimento em 2019 na Copa América na cidade do Rio de Janeiro em que mais uma vez um indivíduo foi preso por erro do reconhecimento facial. A segunda, já declinada em números, é que 90,5% de pessoas presas pelo uso do reconhecimento facial eram consideradas negras (Nunes, 2019) o que enfaticamente demonstra um risco aqui já enfatizado, isto é, o racismo direcionado por essas ferramentas artificiais (Lapin, 2021, p. 38). Se não há uma prestação de contas, não há um controle, motivo pelo qual com o uso massivo torna-se impossível de mensurar estes erros não catalogados.

Ainda em termos práticos, o programa Smart Sampa, iniciado pela Secretaria Municipal de Segurança Urbana junto com a prefeitura de São Paulo, teve o fim de monitorar a cidade por câmeras (Secretaria Municipal de Segurança Urbana, 2024). Na sua instauração, o edital divulgado pela prefeitura foi suspenso sobre denúncias de afirmações preconceituosas como “a pesquisa deve ser feita por diferentes tipos de características como cor, face e outras características” (2023, p.17) além de que o reconhecimento deve decorrer de ações relacionadas atos de “vadiagem” (2023, p.17). O resultado foi que o edital voltou a vigorar normalmente sob a justificativa de que não havia indícios discriminatórios na qualificação de câmeras de monitoramento e mais, que o conhecimento técnico era insuficiente para identificar eventual parcialidade.

Em suma, conclui-se que apesar de uma política pública implantada para fins de segurança pública, há impactos significativos na sociedade, sejam eles sociais, éticos e até mesmo legais. A inserção desta ferramenta de Inteligência artificial é uma realidade, mas os números empíricos sobre seus efeitos não vem sendo exatamente os esperados, de maneira que esse artifício de segurança não vem sendo exatamente para garantir a proteção da população brasileira. Diante disso, permite-se que inicie o próximo capítulo com uma análise das possíveis legislações aptas a contornar este cenário.

2.2 A REGULAÇÃO DO RECONHIIECIMENTO FACIAL NA SEGURANÇA PÚBLICA DO ESTADO DE SÃO PAULO

Riscos foram expostos, mas o principal enfoque detalhado pelo relatório da LAPIN (2021), foi a ausência de transparência e legislação no uso do reconhecimento facial. Deixar a responsabilidade de legislar especificamente sobre o referido assunto para outros entes foi o que o artigo 4, inciso III e § 1º da LGPD fez, permitindo que normas particulares pudessem resguardar sobre as essas inteligências artificiais (de Castro, de Paula, 2022, p. 4 - 2). Diante disso, caberá à este capítulo o objetivo em destrinchar as propostas legislativas que ainda estão em tramitação com a finalidade de buscar uma regulamentação específica que esteja conectada aos ditames desta tecnologia de inteligência artificial.

Partindo de uma linha cronológica e não muito exaustiva, o projeto de Lei nº 9.414/2017 (Brasil, 2017) direciona o tema para o serviço público de transporte, em que o objeto principal é verificar se o indivíduo que está fazendo o uso do serviço é de fato ele mesmo. Neste ponto, o olhar direciona a sua real identidade com o fim de evitar que o passageiro faça usufruto do serviço de maneira irregular, além de registrar o trajeto realizado pelo mesmo (de Castro, de Paula, 2022, p. 4 – 2).

Em contrapartida com um outro olhar o Projeto de Lei nº 9.736/2018 teve seu foco em emendar a Lei nº 7.210/1984, cujo intuito é estabelecer uma vigilância aos indivíduos que estão ou já foram submetidos ao cárcere. Deste modo, o objetivo seria voltado ao controle pela biometria facial para fins de reconhecimento do cidadão encarcerado (Brasil, 2018).

Partindo para um olhar mais cauteloso, Pedro Francisco, Louise Hurel e Mariana Rielli (2020, p. 16) realizam dois apontamentos pertinentes quanto à ambos os projetos. O primeiro é que o teor do reconhecimento é ratificar a identidade do indivíduo, razão pela qual não é preciso de muitas informações ao passo confirmar é menos árduo do que identificar quem é o sujeito.

E segundo que ambos objetivam fomentar a ferramenta artificial em locais específicos, não havendo as preocupações quanto aos riscos expostos anteriormente. Deste modo, ainda que sejam projetos reguladores, a linha de inclusão digital está longe de preocupar com garantias de titulares de dados sensíveis.

Com um cunho mais revolucionário, o deputado federal Bibo Nunes propôs em 2019 o PL nº 4.612/2019, cujas palavras do próprio projeto são "um marco regulatório" (Brasil, 2019). Além do termo inovador, o Projeto de Lei ainda abarca questões, que foram tratadas nesta pesquisa, quais sejam o uso indevido de dados ocasionadores de casos discriminatórios, ao mencionar que a proteção dos dados biométricos deve ser alavancada tanto quanto a evolução das tecnologias artificiais (Brasil, 2019).

Dentro desta mesma órbita o PL ainda cuida de dois pontos que o reconhecimento facial interfere: quais são as formas de tratamento desses dados faciais, como e quando eles serão utilizados. Por fim e não menos importante ressalta que o mais próximo que o projeto de Bibo Nunes chega à segurança pública é o Banco Nacional de Reconhecimento Facial e Emocional (Brasil, 2019). Segundo o art. 7-D, indica-se a possibilidade de uma big data facial e emocional de pessoas que possuem um mandado de prisão em aberto. A polémica está na precisão dos algoritmos, isto é, não apenas em dados biométricos, mas também no reconhecimento facial, caracterizando como de Castro e de Paula (2022, p. 10 – 2) menciona, à uma ressalva não muito clara.

De volta a linha e mais próximo na segurança pública e o reconhecimento facial para fins de vigilância, está o Projeto de Lei nº 3.069/2022 (Brasil, 2022) que torna o uso desta ferramenta de tecnologia artificial a protagonista deste cenário. Ainda que o roteiro tenha sido a aplicação desta política pública na segurança pública, o projeto deixa de se atentar em princípios básicos como a forma do uso de dados captados, a prestação de contas, a necessidade de um relatório indicador de impactos e efeitos e mais, a transparência no seu uso.

Fora dos olhares técnicos do Direito, há grupos no Brasil que se movimentam contra a maré do uso do reconhecimento facial. A iniciativa Tire meu Rosto de sua Mira tem como enfoque o banimento da referida ferramenta (Fachin, Leite, 2023, p.16), contando com o apoio de mais de 50 (cinquenta) organizações. (Tire Meu rosto da Sua Mira, 2022). Ainda extramuros legislativos, o Grupo de Trabalho de Reconhecimento Facial foi formado pelo Conselho Nacional de Justiça solicitado pela associação sem fins lucrativos *Innocence Project Brasil* (Kremer, Costa, 2022, p. 5). O grupo de trabalho, de maneira sucinta, realizou análises voltadas à possível regulamentação do uso do reconhecimento facial no Poder Judicial impossibilitando que pessoas sejam condenadas equivocadamente por decisões automatizadas. A discussão do

grupo aprofundou-se inclusive em um dos temas aqui abordados, indicando que a maior parte de erros reportados no reconhecimento facial está no Estado de São Paulo (Conselho Nacional de Justiça, 2022), este que inclusive tem apenas projetos de lei favoráveis à implantação da referida ferramenta (Tire Meu rosto da Sua Mira, 2022).

Caminhando para o contorno que esta pesquisa está realizando, insta afirmar que apesar da existência projetos de leis federais com intuito a regulamentar o reconhecimento facial, a responsabilidade acaba que é gerenciada pelos Estados, que, além de permitidos pela LGPD, assume a posição de preenchedores de lacunas legislativas (Francisco, Hurel, Rielli, 2020, p.19). São projetos de leis estaduais localizados em regiões do Rio de Janeiro, Goiás, Minas Gerais e Paraná, todos voltados à anuência do uso de tecnologias artificiais.

O Estado de São Paulo (Francisco, Hurel, Rielli, 2020, p.17) está dentre os cinco estados que ainda há projetos de Lei em andamento com o PL nº 865 de 2019, o qual está em tramitação de urgência. Assim como o PL nº 9.414/2017, o Projeto de Lei do Estado do Estado de São Paulo também está direcionado à linhas de locomoção, mais especificamente às Companhias do Metropolitano de São Paulo e da Companhia Paulista de Tren Metropolitano (Brasil, 2019). Com 7 artigos, o objetivo principal foi a vigilância, além de finalidades para coibir abusos sexuais de forma subsidiária. A justificativa, ainda mais sucinta, fundamenta-se na necessidade de manter a segurança interna dos metrôs. Apesar de ser um projeto de lei incentivando o uso da ferramenta, a forma de regulamentação é insuficiente, ao passo que o próprio projeto repassa a responsabilidade ao Poder Executivo (Brasil, 2019).

Uma outra possível regulamentação, no que diz respeito ao já enunciado edital nº15/2024 referente à câmeras corporais compostas com funcionamento de reconhecimento facial, foi a Portaria do Ministérios da Justiça e Segurança Pública nº 648/2024, a qual determinou “diretrizes sobre o uso de câmeras corporais pelos órgãos de segurança pública”. Nestes termos o que merece seu devido destaque são os valores à “transparência, responsabilidade e prestação de contas” e ainda ao “respeito aos direitos e garantias fundamentais” (Brasil, 2019). Uma outra regulamentação na diretriz, a qual estabelece uma função matemática com o risco relacionado à falta de conhecimento técnico de ferramentas artificiais é a obrigação de órgãos de segurança pública em fornecer as devidas instruções sobre as câmeras corporais acompanhadas do reconhecimento facial, bem como realizar pesquisas sobre seu uso e eventuais efeitos (Brasil, 2019). A ênfase negativa está na ausência da menção sobre o reconhecimento facial em si, tendo em vista a imensidão de dados aqui expostos sobre esta ferramenta, mas paradoxalmente ela foi projetada para ser implementada nestas câmaras corporais.

Em face das conclusões permitidas pelas referências expostas, foi possível abordar em segundo lugar sobre as legislações e projetos de leis pertinentes para cuidar do tema. Apesar do artigo 4, inciso III, §1º da LGPD (Brasil. 2018) repassar a responsabilidade de legislar sobre uso da IA no reconhecimento facial como política pública para outros entes (de Castro, de Paula, 2022), ainda não há legislação pertinente sobre o tema. A questão foi os projetos de leis que tinham como fim ora verificar a identidade, ora reconhecer quem era o indivíduo. Porém não houve projetos capazes de detalhar como os dados seriam tratados e como haveria a prestação de contas e a obrigação de uma devida transparência. Demonstrou-se a existência de ações fora do campo do Direito, com organizações e grupos de trabalhos. Contudo, apesar de movimentos contrários e pontuações sobre os riscos, o uso do reconhecimento facial para fins de segurança pública continua florescendo, com 17 capitais do Brasil indicando o interesse na implementação. No Estado de São Paulo há o interesse em implementar câmaras corporais acompanhadas desta ferramenta, mas fundada apenas em diretrizes (DTIC, 2024). Resta identificar quais são os riscos do uso do reconhecimento facial inseridos no uso diário destas câmeras corporais por policiais militares, sem que haja o prejuízo de uma possível inclusão digital na segurança pública.

3 ANÁLISE DO EDITAL E O CONTEXTO E REQUISITOS DAS CÂMARAS CORPORAIS DOS POLICIAIS MILITARES EM SÃO PAULO

Diante dos riscos sobre o reconhecimento facial e as diretrizes e legislações referentes ao seu uso especialmente na segurança pública já debatidas, realiza-se um recorte no que se refere ao edital nº15/2024 (DTIC, 2024) em relação às conclusões extraídas dos dois primeiros capítulos, especialmente no que condiz à aplicação inovadora desta ferramenta em câmeras corporais utilizadas no exercício da função por policiais militares do Estado de São Paulo.

No dia 22 de maio de 2024 o Governo do Estado de São Paulo, mais especificamente a Diretoria de Tecnologia da Informação e Comunicação – DTIC, divulgou o edital de licitação na modalidade de Pregão Eletrônico, nº 90003/24, cujo fim é a contratação de 12 mil câmaras corporais com novas funcionalidades, dentre elas, o reconhecimento facial, a serem utilizadas pela Polícia Militar em meio de sua atuação (DO PORTAL DO GOVERNO, 2024).

Dentro deste roteiro investigatório, o primeiro ponto que merece destaque e que está mais próximo dos riscos relativos ao uso de reconhecimento facial é o tópico “Atribuições da contratada” e “Descrição da Solução”. Em ambas as diretrizes, nos itens 5.4, 15.8.1.21 e seguintes, respectivamente, há a menção da garantia de transferir o conhecimento referente ao

funcionamento do equipamento. Ainda, há a transferência à contratada do encargo em promover treinamentos e manuais de fácil leitura aos operados contratantes (DTIC, 2024). É interessante destacar que não apenas neste item mencionado, mas ao longo do tópico referentes às obrigações da contratada e do tópico "Atividades do Colaborador Alocado" mostra-se o interesse em indivíduos dispostos a operar tecnicamente as câmaras. O edital conta com um tópico especialmente destinado à capacitação de pessoas, determinando no mínimo 10 (dez) policiais militares por treinamento em sede da fabricante, contando com o ensino básico e avançado do sistema operacional. Por ora indica-se a primeira problemática abordada no início desta pesquisa, qual seja, a inexistência ou existência do conhecimento da tecnologia de IA manuseada pelo operador, mas que é motivo de preocupação pela Diretoria de Tecnologia de Informação e Comunicação.

Uma outra demonstração de interesse em delegar domínio sobre o objeto licitado operado com o reconhecimento facial são os termos do tópico "Critérios de medição e pagamento", atribuindo à empresa licitada o dever em expor a forma de manuseio do objeto ofertado, ora quando requisitado, ora no início do contrato (DTIC, 2024). Ocorre que, ainda que o edital se comprometa exaustivamente com a delegação de conhecimento e técnicas para manuseio, os fatos de ferramentas já implementadas como o projeto "Cidade Segura" indicam o contrário, em que a informação na prática não foi devidamente conferida (Lapin, 2021, p. 49).

Por outro lado, no item "Requisitos Gerais da Contratação (15.1) há a exigência de que o produto seja oferecido com a "junção de práticas e padrões que possuem o objetivo de manter os softwares e, quando cabível, os firmwares dos dispositivos atualizados, as atividades de mensuração, análises de desempenho, geração de relatórios gerenciais" (DTIC, 2024). Neste mesmo sentido de exigência de relatórios, há também no item 15.8.1.9, mais especificamente no tópico "Atribuições da contratada" e ainda no tópico "requisitos gerenciamento e custódia", no item 23.5.1, indicando exaustivamente mais de dez tipos de relatórios a serem apresentados pelo software. Acontece que há um limbo entre exigir um equipamento gerador de relatórios gerenciais e realmente fornecer relatórios de impacto à proteção de dados pessoas previstas na LGPD (Brasil, 2018). A título desta observação, a empiria indicada a partir dos vinte e cinco pedidos de informações à autoridades públicas, perfazendo dois à Polícia Civil do Estado de SP, respondidos negativamente, explica que nem sempre uma normativa exigindo um relatório é realmente cumprida, sendo até mesmo desconhecida (Lapin, 2021, p. 49).

Em cenário complementar há também a discussão sobre o armazenamento de dados. No tópico "Critérios de medição e pagamento", já mencionado, a indicação é que os dados de imagens e vídeos captados nas câmeras corporais deverão ser armazenados em 48 (quarenta e

oito) horas no complexo da Polícia Militar do Estado de São Paulo. Quando a estes dados, eles serão armazenados em até 30 (trinta) dias, e só depois podem ser lixados, mantendo-se apenas resquícios originais. Além desse fluxo de informações, o edital conta com um serviço que realiza gravações e transmissões ao vivo, permitindo que o Centro de Operações da Polícia Militar gerencie dados pessoais de todos os indivíduos abordados pela autoridade. Mesmo com a manipulação intensa de dados, mostra-se que o edital, no tópico "requisitos da COP" está sempre atento em mostrar ao titular que estes dados estão sendo captados (DTIC, 2024, p. 53).

Além de sinalizar o seu uso, itens deste mesmo tópico restringem em cuidar de quem terá o acesso a estes dados, indicando expressamente em 19.1.19.2 "O armazenamento interno deverá ser na própria câmera, não podendo ser acessível ao usuário e por pessoas não autorizadas de maneira alguma, sem causar inutilização do equipamento" (DTIC, 2024, p. 53). Entretanto, quando ao manuseio, infere-se um ponto aqui já discutido, isto é, como eles serão tratados na ferramenta de reconhecimento facial e se houver esse fim, se há outra finalidade para qual eles são captados (DTIC, 2024). Para reafirmar ainda mais essa contradição, o edital respeita princípios referentes à proteção de dados, contudo sem afirmar como eles serão de fato tratados, especialmente nos cortes de cena que representam os riscos do reconhecimento facial.

Mesmo com previsão de relatórios, delegações de conhecimento técnico e diretrizes no manuseio de dados pessoais, as câmeras corporais terão também a capacidade de captar as chamadas "snapshots" (DTIC, 2024, p. 57). Com essa sistemática, essas imagens irão compor um complexo indicado pelo licitante e que de forma didática, irá compor um banco de dados auxiliar no chamado programa Muralha Paulista. Para fins de esclarecimento, faz-se necessário realizar um parêntese neste estudo, expondo que o respectivo programa foi implantado pelo Estado de São Paulo, no ano de 2023, caracterizando como uma política pública para fins de vigilância. Dentre outras funcionalidades, o programa conta com a instalação de câmaras de vigilância funcionando a partir da Inteligência artificial e consequentemente do reconhecimento facial, cujo fim é o combate à ações criminosas (Brasil, 2024).

Além desta fragilidade referente ao reconhecimento facial, o edital indica que o software deve dispor de "tecnologia de Inteligência Artificial, que permita o reconhecimento automático de padrões e formas para identificar e classificar objetos, como pessoas, veículos e caracteres com subtipos no campo de visão da câmera" (DTIC, 2024, p.65). Não só, mas o edital deixa em aberto a quem caberá introduzir a ferramenta de reconhecimento facial operacionalizada pela Inteligência Artificial, ora implantada na própria câmera, ora no software que a acompanha. Para agravar ainda mais o cenário, o roteiro do documento conta ainda com a possibilidade de inserir informações externas até mesmo de um celular e mais, estabelecer o

pareamento de pessoas a partir de “cútis, cor do cabelo, cor da roupa, camisas, calça e objetos” (DTIC, 2024, p. 65).

Deste modo, a congruência é que as câmeras corporais serão responsáveis por captar imagens durante seu funcionamento, das quais serão base para reconhecer informações dentro de um banco de dados. Estes por sua vez irão fazer parte de um servidor utilizado pelo Programa Muralha Paulista, especialmente no funcionamento de reconhecimento e no momento de acionar alarmes de infração (DTIC, 2024, p. 57). Não só, mas as câmeras operacionais serão compostas pela inteligência artificial capaz de realizar o reconhecimento de pessoas a armas (DTIC, 2024). Em face desse cenário, e sem regulação específica, o pesquisador Pablo Nunes, em uma entrevista à CBN, demonstra certa agonia indicando que há uma problemática em instalar uma ferramenta de reconhecimento facial, com os riscos aqui já assinalados, em uma câmera corporal conduzida por um policial militar, não havendo uma aplicação prática similar em qualquer sistema de vigilância pública no mundo (Reis, 2024).

Finda-se o raciocínio afirmando que a aplicação de cidades inteligentes em um cenário de políticas públicas é o que o Estado tem por fim em face de um crescimento da população e a necessidade de garantir o bem-estar social digitalmente inclusivo. Ocorre que nada adianta implementar ferramentas fundadas na inteligência artificial no âmbito de Tecnologia da Informação e Comunicação se não há estudos precisos sobre seus riscos e sobre regulamentações. Não somente, mas insistir ainda mais na melhoria de uma ferramenta de inteligência artificial que demonstra efeitos negativos é resolver um problema, mas criar outros cinco ainda maiores, dificultando ainda mais uma política digitalmente inclusiva.

CONCLUSÃO

A pesquisa teve como objetivo analisar o uso de reconhecimento fácil na segurança pública destacando os desafios e preocupações legais, técnicas e sociais, especialmente no contexto do Estado de São Paulo.

Inicialmente se tratou a respeito dos riscos e violações do uso do reconhecimento facial, detalhando os riscos associados ao reconhecimento fácil, incluindo a violação de privacidade, erros de identificação e discriminação racial, ilustrando com exemplos reais como o do Carnaval de 2019 no Rio de Janeiro.

No capítulo seguinte se tratou da regulação do reconhecimento fácil na Segurança Pública no Estado de São Paulo, focando a discussão na ausência de regulamentação específica

e nas iniciativas legislativas em andamento, destacando a necessidade de leis claras e rigorosas para regular o uso da tecnologia

No capítulo final, analisou-se o edital e o contexto e requisitos das câmeras corporais dos policiais militares em São Paulo, verificando o Edital n. 15/2024, que tem como finalidade a implementação de cames corporais com reconhecimento fácil, discutindo suas exigências, limitações e os potenciais impactos sociais e legais.

Teve-se como pergunta central os riscos relacionados à tecnologia de reconhecimento facial em câmeras utilizadas pela segurança pública e de quais maneiras se poderia mitigar tais riscos. Os principais riscos identificados incluem a violação de direitos fundamentais como privacidade e proteção de dados, erros de identificação e discriminação racial. Esses riscos podem ser mitigados por meio de regulações específicas, transparência, controle rigoroso no uso das tecnologias e treinamento adequado dos operadores.

O estudo atendeu aos objetivos ao identificar e analisar os riscos e ao propor que regulamentações específicas e transparência são essenciais para mitigar esses riscos. Isso foi possível em atendimento aos objetivos específicos, analisando a legislação atual e projetos de lei relacionados ao reconhecimento facial, identificando lacunas e propondo a necessidade de regulamentações detalhadas e específicas. Fora discutido os impactos éticos e sociais, com ênfase na discriminação racial e violação de privacidade. Analisou-se exemplos concretos, como os erros de reconhecimento durante o Carnaval de 2019, no Rio de Janeiro. Por fim, sugeriu-se diretrizes para regulamentação, com a necessidade de maior transparência e controle, além de treinamento adequado dos policiais que deverão operar a tecnologia.

Além do mais, as hipóteses propostas, relacionadas a possíveis violações de direitos fundamentais, falta de regulamentação aumentando os riscos e a implementação adequada de normas para poder mitigar tais riscos, foram confirmadas com a pesquisa.

Assim sendo, conclui-se que o uso do reconhecimento facial na segurança pública apresenta significativos riscos de violação de direitos fundamentais, erros de identificação e discriminação racial. Esses riscos podem ser mitigados com regulamentação específica, maior transparência operacional dos dados e controle no uso das tecnologias, além de treinamento adequado. É esse4cnail que os legisladores e gestores públicos considerem essas recomendações para assegurar o uso ético e eficiente da tecnologia de reconhecimento facial, protegendo direitos dos cidadãos e promovendo a segurança pública de forma inclusiva e justa.

REFERÊNCIAS

BRASIL, Câmara dos Deputados. **Projeto de Lei nº 9.414, de, 19 de dezembro de 2017**. Obriga a instalação da leitura de impressão digital e facial nos meios de transportes públicos coletivos. Brasília: Câmara dos Deputados, 2017. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2166846&ficha Amigavel=nao. Acesso em: 04 jun. 2019

BRASIL, Câmara dos Deputados. **Projeto de Lei nº 9.736, de, 07 de março de 2018**. Acrescenta dispositivo à Lei nº 7.210, de 11 de julho de 1984, para incluir a previsão de identificação por reconhecimento facial. Brasília: Câmara dos Deputados, 2017. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2169011&ficha Amigavel=nao. Acesso em: 04 jun. 2019

BRASIL, Câmara dos Deputados. **Projeto de Lei nº 4.612, de, 21 de agosto de 2019**. Dispõe sobre o desenvolvimento, aplicação e uso de tecnologias de reconhecimento facial e emocional, bem como outras tecnologias digitais voltadas à identificação de indivíduos e à predição ou análise de comportamentos. Brasília: Câmara dos Deputados, 2017. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2216455. Acesso em: 04 jun. 2019

BRASIL, Câmara dos Deputados. **Projeto de Lei nº 3.069, de, 22 de dez de 2022**. Dispõe sobre o uso de tecnologia de reconhecimento facial automatizado no âmbito das forças de segurança pública e dá outras providências. Brasília: Câmara dos Deputados, 2017. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2345261&ficha Amigavel=nao#:~:text=PL%203069%2F2022%20Inteiro%20teor,Projeto%20de%20Lei&text =Disp%C3%B5e%20sobre%20o%20uso%20de,p%C3%BAblica%20e%20d%C3%A1%20ou tras%20provid%C3%AAncias.&text=Disciplinamento%2C%20tecnologia%2C%20Reconhec imento%20facial%2C,%C3%A2mbito%2C%20Seguran%C3%A7a%20P%C3%BAblica%2C %20diretrizes.. Acesso em: 04 jun. 2019

BRASIL, Câmara dos Deputados. **Projeto de Lei nº 21, de 30 de set de 2021**. Estabelece fundamentos, princípios e diretrizes para o desenvolvimento e a aplicação da inteligência artificial no Brasil; e dá outras providências. Brasília: Câmara dos Deputados, 2021. Disponível em: https://www25.senado.leg.br/web/atividade/materias/-/materia/151547#:~:text=Projeto%20de%20Lei%20n%C2%B0%2021%2C%20de%202020& text=Ementa%3A,Brasil%3B%20e%20d%C3%A1%20outras%20provid%C3%AAncias.. Acesso em: 04 jun. 2019

BRASIL, Câmara dos Deputados. **Projeto de Lei nº 1.515, de, 07 de junho. de 2022**. Lei de Proteção de Dados Pessoais para fins exclusivos de segurança do Estado, de defesa nacional, de segurança pública, e de investigação e repressão de infrações penais. Brasília: Câmara dos Deputados, 2017. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2326300&ficha Amigavel=nao. Acesso em: 04 jun. 2019

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF, [2018]. Disponível em:

https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 02 jun 2024.

BRASIL. Lei nº 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Brasília, DF, [2018]. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 02 jun 2024

BRASIL. Ministério da Justiça e Segurança Pública. Portaria nº 648, de 28 de maio de 2024. Estabelece diretrizes sobre o uso de câmeras corporais pelos órgãos de segurança pública. Brasília, DF, 2024. Disponível em: https://www.gov.br/mj/pt-br/assuntos/noticias/201csalto-civilizatorio201d-diz-lewandowski-sobre-novas-diretrizes-de-uso-de-cameras-corporais. Acesso em: 02 jun 2024

BRASIL, Agência. Governo de SP amplia programa de integração de sistemas de vigilância. **Veja São Paulo**, São Paulo, 22 mai. 2024. Disponível em: https://vejasp.abril.com.br/cidades/governo-sp-programa-muralha-paulista. Acesso em: 17 jun. 2024.

CONSELHO NACIONAL DE JUSTIÇA. Grupo De Trabalho "Reconhecimento De Pessoas". **Exposição e análise dos dados coletados.** Brasília, DF: Conselho Nacional de Justiça, 2022.

COSTA, Ramon Silva; NEGRI, Sergio Marcos Carvalho de Ávila; DE OLIVEIRA, Samuel Rodrigues. O Uso de Tecnologias de Reconhecimento Facial Baseadas em Inteligência Artificial e o Direito à Proteção de Dados. Assunto Especial: Proteção de Dados e Inteligência Artificial: Perspectivas Éticas e Regulatórias. Brasília, DF, v 17, n. 93, p. 82-103, maio/ jun. 2020. Disponível em: https://www.portaldeperiodicos.idp.edu.br/direitopublico/article/view/3740/Negri%3B%20Oliveira%3B%20Costa%2C%202020. Acesso em: 02 jun 2024.

COSTA, Ramon Silva; Kremer, Bianca. Inteligência artificial e discriminação: Desafios e perspectivas para a proteção de grupos vulneráveis diante das tecnologias de Reconhecimento facial. Direitos Fundamentais & Justiça, Belo Horizonte, n 16, p. 145-167, out. 2022. Disponivel em: https://dfj.emnuvens.com.br/dfj/article/view/1316. Acesso em: 30 nov 2023.

DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO. Edital de licitação nº 15/2024. Pregão Eletrônico nº 90003/24. [Contratação de empresa especializada para prestação de serviço, de solução integrada de gestão, captação, transmissão, armazenamento, custódia e compartilhamento, de vestígios evidências e provas digitais por câmeras operacionais portáteis nas atividades policiais.]. **Diretoria de Tecnologia da Informação e Comunicação**: órgão da Polícia Federal, DTIC, 21 Mai 2024.

FACHIN, Zulmar Antonio; LEITE, Natalia Battini Simões. Vigilância Automatizada: A Utilização Do Reconhecimento Facial Para Fins De Segurança Pública E O Tratamento Da Lei Geral De Proteção De Dados. Conselho Nacional de Pesquisa e Pós-Graduação em Direito - CONPEDI, Florianópolis, Santa Catarina. ISBN: 978-65-5648-764-9. Disponível em: www.conpedi.org.br. Acesso em: 02 jun 2024.

INSTITUTO IGARAPÉ. **Reconhecimento Facial no Brasil,** 2019. Disponível em: https://igarape.org.br/infografico-reconhecimento-facial-no-brasil/. Acesso em: 02 jun 2024

INSTITUTO IGARAPÉ. **Videomonitoramento,** 2019. Disponível em: https://igarape.org.br/infografico-reconhecimento-facial-no-brasil/. Acesso em: 02 jun 2024

NUNES, Pablo. Novas ferramentas, velhas práticas: reconhecimento facial e policiamento no Brasil. Rede de Observatórios da Segurança. p. 69 – 72, jun-out, 2019. Disponível em: https://cesecseguranca.com.br/wp-content/uploads/2019/11/Rede-de-Observatorios_primeiro-relatorio_20_11_19.pdf. Acesso em: 02 jun 2024.

NUNES, Pablo. Monitor de novas tecnologias na segurança pública no Brasil. **O panóptico.** Disponível em: https://www.opanoptico.com.br/#mapa. Acesso em: 02 jun 2024.

NUNES, Pablo. Levantamento revela que 90,5% dos presos por monitoramento facial no brasil são negros. **Centro de Estudos de Segurança e Cidadania.** Disponível em: https://cesecseguranca.com.br/artigo/levantamento-revela-que-905-dos-presos-por-monitoramento-facial-no-brasil-sao-negros/. Acesso em: 02 jun 2024.

Programa Smart Sampa avança na capital com 10 mil câmaras em funcionamento. **Cidade de São Paulo. Secretaria Municipal de Segurança Urbana.** São Paulo, ano 2024, 25 abr. Disponível em: https://capital.sp.gov.br/w/programa-smart-sampa-avan%C3%A7a-na-capital-com-10-mil-c%C3%A2meras-em-funcionamento#:~:text=Atualmente%20a%20cidade%20de%20S%C3%A3o,Civil%20e%20Militar%2C%20dentre%20outros. Acesso em: 09 jun. 2024

DO PORTAL DO GOVERNO. Governo de SP publica edital para ampliar uso de câmeras corporais na PM. **Governo do Estado de São Paulo**, São Paulo, 22 mai. 2024. Disponível em: https://www.saopaulo.sp.gov.br/spnoticias/ultimas-noticias/governo-de-sp-publica-edital-para-ampliar-uso-de-cameras-corporais-na-pm/. Acesso em: 02 jun 2024

REIS, Carolina; ALMEIDA, Eduarda; DA SILVA; Felipe; DOURADO, Fernando. **Relatório sobre o uso de tecnologias de reconhecimento facial e câmeras de vigilância pela administração pública no Brasil**. Brasília: Laboratório de Políticas Públicas e Internet, 2021.

REIS, Daniel. Governo de SP quer contratar câmeras corporais com reconhecimento facial para PM. **CBN.Globo**. São Paulo, 10 mai. 2024. Disponível em: https://cbn.globo.com/sao-paulo/noticia/2024/05/10/governo-de-sp-quer-contratar-cameras-corporais-com-reconhecimento-facial-para-pm.ghtml. Acesso em: 17 jun. 2024

ORGANIZAÇÃO TIRE MEU ROSTO DA SUA MIRA. Brasília, 2022. Disponível em: https://tiremeurostodasuamira.org.br. Acesso em: 02 jun 2024.