



**UNIVERSIDADE ESTADUAL DA PARAÍBA  
CAMPUS I  
CENTRO DE CIÊNCIAS JURÍDICAS  
DEPARTAMENTO DE DIREITO PÚBLICO  
CURSO DE DIREITO**

**CAROLINA ALYS CARVALHO DUARTE**

**IMPLICAÇÕES JURÍDICAS DO USO DO RECONHECIMENTO FACIAL NO  
MUNICÍPIO DE CAMPINA GRANDE – PB**

**CAMPINA GRANDE – PB**

**2020**

CAROLINA ALYS CARVALHO DUARTE

**IMPLICAÇÕES JURÍDICAS DO USO DO RECONHECIMENTO FACIAL NO  
MUNICÍPIO DE CAMPINA GRANDE – PB**

Artigo Científico apresentado ao Centro de Ciências Jurídicas, Campus I, Universidade Estadual da Paraíba, como requisito parcial para obtenção do Título de Bacharel em Direito.

Área de concentração: Ciências Criminais e Novas  
Tecnologias.

Orientadora: Prof.<sup>a</sup> Dr.<sup>a</sup> Aureci Gonzaga Farias.

CAMPINA GRANDE – PB

2020

É expressamente proibido a comercialização deste documento, tanto na forma impressa como eletrônica. Sua reprodução total ou parcial é permitida exclusivamente para fins acadêmicos e científicos, desde que na reprodução figure a identificação do autor, título, instituição e ano do trabalho.

D812i Duarte, Carolina Alys Carvalho.  
Implicações jurídicas do uso do reconhecimento facial no município de Campina Grande – PB [manuscrito] / Carolina Alys Carvalho Duarte. - 2020.  
21 p.  
Digitado.  
Trabalho de Conclusão de Curso (Graduação em Direito) - Universidade Estadual da Paraíba, Centro de Ciências Jurídicas, 2020.  
"Orientação : Prof. Dr. Aureci Gonzaga Farias .  
Coordenação do Curso de Direito - CCJ."  
1. Criminologia. 2. Segurança pública. 3. Reconhecimento facial. I. Título  
21. ed. CDD 345.02

CAROLINA ALYS CARVALHO DUARTE

**IMPLICAÇÕES JURÍDICAS DO USO DO RECONHECIMENTO FACIAL NO  
MUNICÍPIO DE CAMPINA GRANDE – PB**

Artigo Científico apresentado ao Centro de Ciências Jurídicas, Campus I da Universidade Estadual da Paraíba, como requisito parcial para obtenção do Título de Bacharel em Direito.

Aprovada em: 02 / 12 / 2020.

BANCA EXAMINADORA

*Aureci Gonzaga Farias*

Professora Dr<sup>a</sup>. Aureci Gonzaga Farias (Orientadora)  
Universidade Estadual da Paraíba (UEPB)

*Raissa de Lima e Melo*

Prof<sup>a</sup>. Me. Raissa de Lima e Melo (UEPB)

MONICA LUCIA  
CAVALCANTI DE

Prof<sup>a</sup>. Dr<sup>a</sup>. Monica Lúcia Cavalcanti de Albuquerque Duarte Mariz-Nóbrega (UEPB)

ALBUQUERQUE  
DUARTE MARIZ  
NOBREGA

Assinado de forma  
digital por MONICA  
LUCIA CAVALCANTI DE  
ALBUQUERQUE  
DUARTE MARIZ  
NOBREGA  
Dados: 2020.12.03  
17:33:41 -03'00'

## **AGRADECIMENTOS**

Agradeço a Deus por não me deixar fraquejar em momentos em que pensei não conseguir chegar até aqui.

Agradeço especialmente à minha Mãe Deuzair e minha avó Teresa, por todo amor, incentivo, apoio e compreensão nestes anos de curso, sem elas nada disso estaria se concretizando.

Agradeço à Professora Aureci Gonzaga Farias que não mediu esforços para a orientação do presente Artigo e por todo seu apoio, atenção, direcionamento e carinho.

Agradeço ao meu esposo, Júnior, pelo seu incentivo, amor e companheirismo de sempre.

E, por último, mas não menos importante, agradeço aos meus amigos; aos que fiz na universidade e fora dela, sem dúvida eles tornaram essa caminhada mais leve.

Tudo o que temos de decidir é o que fazer com o tempo que nos é dado.

(Senhor dos Anéis – A sociedade do anel – J.R.R. Tolkien).

# IMPLICAÇÕES JURÍDICAS DO USO DO RECONHECIMENTO FACIAL NO MUNICÍPIO DE CAMPINA GRANDE – PB

DUARTE, Carolina Alys Carvalho<sup>1</sup>

## RESUMO

A biometria facial vem sendo utilizada em larga escala, nos últimos anos, em todo o mundo, com a sua aplicação variando desde o uso pessoal (por exemplo, para desbloquear *smartphones*) até o uso pelos governos e seus órgãos de segurança pública, para vigilância e investigações criminais. Os dados de imagem coletados não necessitam de contato direto do indivíduo com o sistema, sendo, portanto, de fácil captação e sigilo. Assim, a legalidade desses sistemas tem sido questionada em diferentes locais, especialmente em função da inexistência de normatização do seu uso, trazendo o risco de serem afetados direitos fundamentais dos indivíduos. Outrossim, este artigo tem, como objetivo central, analisar de que forma a adoção da tecnologia de reconhecimento facial trouxe avanços na segurança pública, de forma geral e, mais especificamente, no município de Campina Grande. A pesquisa realizada caracterizou-se, quanto aos fins, como *exploratória*, visto que a temática possui pouco conhecimento acumulado e sistematizado; e, quanto aos meios, como *bibliográfica*, por basear-se em material publicado em livros, revistas, jornais, redes eletrônicas. Foram utilizados os métodos *observacional* e *fenomenológico*, de maneira a permitir a análise do reconhecimento facial no cerne da sua aplicação. A utilização da tecnologia de reconhecimento facial, na área de segurança pública, apresenta bons resultados, principalmente em relação às prisões efetuadas e ao monitoramento de eventos públicos. No entanto, há responsabilidades éticas a serem consideradas, tornando imprescindível a regulação da aplicação dessa tecnologia, a fim de garantir que seja segura e eficiente para todos.

Palavras-chave: Reconhecimento Facial, Regulação, Segurança Pública.

---

<sup>1</sup> Concluinte do Curso de Bacharelado em Direito pela Universidade Estadual da Paraíba.

# **IMPLICAÇÕES JURÍDICAS DO USO DO RECONHECIMENTO FACIAL NO MUNICÍPIO DE CAMPINA GRANDE – PB**

DUARTE, Carolina Alys Carvalho<sup>1</sup>

## **ABSTRACT**

In recent years facial biometrics have been used on a large scale all over the world. Its application ranges from personal use (e.g. to unlock smartphones) to governmental use (by law enforcement agencies) for surveillance and criminal investigations. The image data collected does not require direct contact of the individual with the system, and is of easy capture and secrecy. Thus, the legality of these systems has been questioned in different places, especially due to the lack of legal rules to discipline their use, which brings the risk of affecting individuals' fundamental rights. Therefore, this article's central objective is to analyze how the adoption of facial recognition technology brought advances in public security, in general and, more specifically, in the municipality of Campina Grande. The research was characterized, as for the purposes, as exploratory, since the theme has little accumulated and systematized knowledge; and, as for the means, as a bibliographic one, for relying on material published in books, magazines, newspapers, electronic networks. The use of observational and phenomenological methods allowed the analysis of facial recognition at the heart of its application. Utilizing facial recognition technology in the public security area has presented good results, particularly in relation to arrests made and the monitoring of public events. Nevertheless, there are ethical responsibilities to be considered, making it essential to regulate the technology application, in order to ensure its safety and efficiency for all.

Keywords: Facial Recognition, Regulation, Public Security.

---

<sup>1</sup> Concluinte do Curso de Bacharelado em Direito pela Universidade Estadual da Paraíba.

## SUMÁRIO

<b>1</b>	<b>INTRODUÇÃO.....</b>	<b>8</b>
<b>2</b>	<b>O RECONHECIMENTO FACIAL AUTOMATIZADO.....</b>	<b>9</b>
<b>3</b>	<b>SEGURANÇA PÚBLICA E O USO DAS NOVAS TECNOLOGIAS.....</b>	<b>11</b>
<b>4</b>	<b>USO DE RECONHECIMENTO FACIAL EM CAMPINA GRANDE – PB ..</b>	<b>13</b>
<b>5</b>	<b>RISCOS DO USO DO RECONHECIMENTO FACIAL .....</b>	<b>14</b>
<b>6</b>	<b>CONSIDERAÇÕES FINAIS .....</b>	<b>17</b>
	<b>REFERÊNCIAS .....</b>	<b>19</b>

## 1 INTRODUÇÃO

A biometria facial é uma categoria de *software* – que mapeia matematicamente as características faciais de um indivíduo e as armazena como uma impressão facial – que vem sendo utilizada em larga escala, nos últimos anos, em todo o mundo. Sua aplicação varia desde o uso pessoal (por exemplo, para desbloquear *smartphones*) até o uso pelos governos e seus órgãos de segurança pública, para vigilância e investigações criminais.

Assim, essa captação de imagens, em tempo real, está hoje no dia a dia das pessoas, seja nos condomínios onde residem, em lojas e transportes públicos, ou em eventos abertos ao público – a exemplo do Carnaval das cidades do Rio de Janeiro e Salvador e das festas juninas de Campina Grande –, para captar padrões comportamentais.

Observe-se que os dados de imagem, coletados pelos sistemas de biometria facial, não necessitam de contato direto do indivíduo com o sistema, sendo, portanto, de fácil captação e sigilo. Assim, a legalidade desses sistemas tem sido questionada em diferentes locais (tendo sido proibido o seu uso em alguns países e cidades), especialmente em função da inexistência de normatização do seu uso, visto que as principais áreas de utilização são a segurança pública e a logística comercial, trazendo o risco de serem afetados direitos fundamentais dos indivíduos. Desta forma, é imprescindível que o Direito e os seus operadores busquem formas de proteger a sociedade de possíveis danos jurídicos.

O interesse desta autora pelo assunto surgiu, principalmente, em aulas do componente curricular Direito e Tecnologia da Informação, com a referência ao reconhecimento facial; a posterior disponibilização de um *podcast* – arquivo digital de áudio transmitido através da Internet –, contendo entrevista a um representante da segurança pública do Estado da Paraíba, trazendo mais esclarecimentos e resultados sobre a utilização dessa tecnologia no município de Campina Grande, durante as festas juninas; e os necessários questionamentos sobre quando, onde e como esse dado pessoal seria tratado e utilizado e, também, se estariam sendo resguardados o direito de imagem, o direito à privacidade, os direitos do consumidor e a proteção de dados pessoais na rede de computadores (recentemente regulamentada pela Lei nº 13.709 de 14 de agosto de 2018 — Lei Geral de Proteção de Dados Pessoais), ainda que para fins de segurança pública.

Tais questionamentos induziram a escolha do tema como objeto de estudo, de maneira que o presente artigo, intitulado “Implicações jurídicas do uso do reconhecimento facial no município de Campina Grande”, tem, como objetivo central, analisar de que forma a adoção da tecnologia de reconhecimento facial trouxe avanços na segurança pública, de forma geral e, mais especificamente, no município de Campina Grande.

A pesquisa realizada caracterizou-se, quanto aos fins, como *exploratória*, visto que a temática possui pouco conhecimento acumulado e sistematizado; e, quanto aos meios, como *bibliográfica*, por basear-se em material publicado em livros, revistas, jornais, redes eletrônicas. Foram utilizados os métodos *observacional* e *fenomenológico*, de maneira a permitir a análise do reconhecimento facial no cerne da sua aplicação – coleta de imagens faciais biométricas de pessoas –, a qual ocorre, geralmente, sem autorização prévia e sem que haja qualquer mecanismo que a normatize, até o momento.

Outrossim, no exercício de utilização, a tecnologia pode levar a dúvidas quanto ao seu *modus operandi* e acabar por atingir, de forma negativa, os direitos básicos daqueles que são os destinatários finais neste contexto: a sociedade. Questiona-se, portanto: “a tecnologia de reconhecimento facial é um sistema que traz benefícios reais aos que a ela se submetem?”

## **2 O RECONHECIMENTO FACIAL AUTOMATIZADO**

A Inteligência Artificial (I.A.) é “um ramo da Ciência da Computação cujo interesse é fazer com que os computadores pensem ou se comportem de forma inteligente” (GOMES, 2010, p. 239). Portanto, é um tipo de inteligência produzida pelo homem, para beneficiar as máquinas com algum tipo de habilidade que simula a inteligência natural do homem. E reconhecer pessoas é uma delas.

O reconhecimento facial é um sistema – desenvolvido, em 1964, por Woodrow Wilson Bredsoe, em conjunto com Helen Chan Wolf e Charles Bisson– cujo objetivo é identificar as pessoas, através de imagem ou vídeo. Tem sido estudado e pesquisado de forma ativa, a partir da década de 1970, inicialmente com uma abordagem fundamentada em características, definindo uma representação com base em proporções da distância, área e ângulo (VIANA *et al.*, 2019, p. 443).

É grande a variedade de técnicas, métodos e conceitos que são utilizados na construção dos sistemas de reconhecimento facial propriamente ditos, mas, de forma geral, estes se constituem em um processo de captação de dados de imagem que utiliza, de forma basilar, uma câmera e um equipamento que realiza inúmeros processos para captar, armazenar, identificar e comparar imagens em um banco de dados.

Silva e Cintra (2015, p. 1) afirmam que o reconhecimento facial é uma técnica biométrica, com a capacidade de reconhecer pessoas por suas características faciais, identificando padrões como formato da boca, do rosto, distância dos olhos, entre outros, e explicam que:

Um humano é capaz de reconhecer uma pessoa familiar, mesmo com muitos obstáculos como distância, sombras, ou apenas a visão parcial do rosto. Uma máquina, no entanto, precisa realizar inúmeros processos para detectar e reconhecer um conjunto de padrões específicos, para rotular uma face como conhecida ou desconhecida. Para isso, existem métodos capazes de detectar, extrair e classificar as características faciais, fornecendo um reconhecimento automático de pessoas.

Para Nunes (2015, p. 36), o reconhecimento facial “é uma tecnologia mais avançada e se baseia em algoritmos, por exemplo o *Eigenfaces*, que mapeia as características do rosto de uma pessoa em um espaço multidimensional”. A autora afirma, ainda, que os computadores podem realizar buscas em bases de dados faciais e/ou efetuarem verificações ao vivo, um-a-um ou um-para-muitos, com uma precisão sem precedentes e o processamento em uma fração de segundo.

Lohn (2012, p. 64) explica que um sistema de reconhecimento facial “mapeia o rosto e gera uma assinatura facial, um código numérico específico para aquela determinada face”. Este código é que é armazenado em banco(s) de dados e utilizado para as buscas, não as fotos em si. Isto permite o armazenamento de milhões de informações de fotos a um baixo custo, bem como uma consulta muito rápida a esses dados.

Marasciulo (2020) trouxe dados de uma pesquisa realizada pela *Surfshark* – empresa que desenvolve ferramentas de proteção de privacidade na Internet –, a qual revelou que, atualmente, 98 (noventa e oito) países usam tecnologias de reconhecimento facial em algum tipo de vigilância pública. Divulgado em maio deste ano, o levantamento baseou-se em dados de 194 (cento e noventa e quatro) países e apontou que, “além dos que já utilizam, 12 (doze) aprovam, mas ainda não

implementaram esse tipo de tecnologia; 13 (treze) consideram utilizá-la; 68 (sessenta e oito) não usam; e 3 (três) a proíbem”. A pesquisa também detectou o uso desses sistemas em 92% (noventa e dois por cento) dos países da América do Sul, a maior porcentagem entre os continentes.

Em 2020, o mundo foi afetado, de forma inesperada, por uma pandemia e, diante de tantas crises anunciadas – como, por exemplo, o colapso do setor de saúde e uma possível crise econômica grave –, governos de todos os países estão empenhados em encontrar alternativas de combate ao vírus. Neste contexto, alguns países, como Rússia e China, se socorrem da tecnologia de reconhecimento facial, para garantir que pessoas infectadas não quebrem o isolamento social ou não deixem de utilizar máscara nos ambientes públicos.

No Brasil, o reconhecimento facial é uma realidade desde 2011, e vem sendo utilizado por diversos tipos de setores, sejam eles privados ou públicos, e, de forma acentuada, pelos órgãos de segurança pública em vários Estados do país. O Instituto Igarapé registrou, até maio de 2019, a utilização dessa tecnologia por autoridades públicas no Brasil, de forma reportada, em 48 (quarenta e oito) situações; destas, 13 (treze) tinham, como principal objetivo, a segurança pública (FRANCISCO *et al.*, 2020, p. 2).

É importante ressaltar que, mesmo já sendo utilizada em diferentes setores, a tecnologia de reconhecimento facial ainda necessita de desenvolvimento para se tornar mais precisa; no entanto, embora possam ocorrer erros de identificação, no momento de reconhecer alguns padrões, “o emprego da ferramenta não deixa de ser algo extremamente útil” (BATISTA *et al.*, 2017, p. 56).

### **3 SEGURANÇA PÚBLICA E O USO DE NOVAS TECNOLOGIAS**

Em uma ótica tradicionalista, a função maior do Estado é prestar segurança aos seus cidadãos, “garantindo-lhes a sua incolumidade física e moral, reflexo de uma convivência pacífica e harmoniosa entre os indivíduos”. Sob esse prisma, portanto, o conceito de segurança pública “está ligado ao de poder de polícia, estando a ordem pública assimilada à ordem interna do grupo” (JUCÁ, 2002, p. 1).

Segundo essa autora, com o surgimento do Estado Democrático de Direito, tal premissa foi remodelada e surgiu o aspecto moderno, trazendo um conceito diferenciado de segurança pública, situando-a em todos os campos da vida humana,

em níveis nacional e internacional, e fazendo o poder de polícia passar a incorporar valores sociais.

A Constituição da República Federativa do Brasil, de 1988, dispõe, em seu artigo 144, que a segurança pública é dever do Estado, direito e responsabilidade de todos, exercida para a preservação da ordem pública e da incolumidade das pessoas e do patrimônio. É um conceito amplo, não se limitando ao combate à criminalidade ou à atividade policial em si: a segurança pública abarca, também, o dever de atuação estatal para que os cidadãos possam conviver, trabalhar, produzir e se divertir, protegendo-os dos riscos a que estão expostos (HELOU, 2008, p. 10).

Conforme afirmam Viana *et al.* (2019, p.438), nos dias atuais, com as mudanças nas demandas, se fazem necessárias novas ferramentas para o bom funcionamento do poder de polícia e da própria segurança pública, de modo que:

Uma das medidas na área de segurança pública é a adoção de novas tecnologias voltadas para a prevenção geral de delitos, pois a prevenção especial salvaguardada na Legislação Penal demonstra-se insuficiente para fazer frente à crescente constatação de maiores ocorrências criminais, fato estudado pela criminologia. Assim, através da Secretaria de Segurança Pública do Estado da Bahia, foi adotada como política pública a tecnologia de reconhecimento facial.

De acordo com Almeida (2009, p. 53), muitas são as áreas de aplicação do reconhecimento facial, dentre elas: ações contra o terrorismo; no controle parlamentar; no controle da circulação; na busca de crianças desaparecidas em meio a multidões; na segurança residencial; na verificação da identidade dos eleitores; nas atividades bancárias; entre outras. Porém, é na segurança pública que sua implantação é mais requerida.

Lobato *et al.* (2020) informam que a expansão das atividades de vigilância urbana costuma ser vista como resposta lógica e necessária ao problema da violência, pois, com frequência, essas tecnologias servem como aliadas na segurança pública, expandindo a “visão” do policial que, “dos centros de operações, monitora as imagens captadas nas diferentes ruas de um bairro, otimizando o uso dos recursos disponíveis diante das limitações enfrentadas em muitos batalhões”. Ainda segundo esses autores, a utilização deste recurso pode ser um aliado em ações que visem coibir tipos específicos de crimes (roubos e furtos, por exemplo) e identificar foragidos da justiça; em alguns casos, pode também auxiliar na identificação de pessoas desaparecidas, embora de modo limitado.

No Brasil, como informa Silva (2020): (a) um dos principais sistemas de reconhecimento facial para segurança pública é o do Estado de São Paulo: adotado pela Polícia Civil, o sistema compara imagens de câmeras (ou de celulares de testemunhas), acessadas por policiais, com uma base de dados com mais de 30 milhões de RGs emitidos no Estado; (b) o Estado da Bahia adotou a tecnologia de reconhecimento facial, para fins de segurança pública, em dezembro de 2018 e, em setembro de 2020, o sistema já havia auxiliado na prisão de 194 (cento e noventa e quatro procurados), apesar da ocorrência de alguns “*falso positivos*”; (c) em 2018, o Estado do Rio de Janeiro começou a testar uma tecnologia de reconhecimento em tempo real, com bons resultados, embora erros tenham acontecido; (d) desde 2019, o Estado do Ceará conta com um aplicativo que permite fazer a busca pela face de indivíduos que estão sem identificação, durante abordagens; (e) a partir de 2018, os sistemas de reconhecimento facial também foram adotados por vários governos municipais, como os de Vitória - ES, João Pessoa - PB, Campina Grande - PB, São José dos Campos - SP, Guarujá - SP, Mesquita - RJ, Blumenau - SC e Pilar - AL, entre outros.

Embora, de forma geral, os resultados obtidos pelo uso da tecnologia de reconhecimento facial sejam considerados bons, Silva (2020) enfatiza a ausência de maiores informações sobre esses resultados, o que impede “análises mais detalhadas sobre as ferramentas de diferentes governos”.

#### **4 USO DE RECONHECIMENTO FACIAL EM CAMPINA GRANDE – PARAÍBA**

O reconhecimento facial foi utilizado no município de Campina Grande - PB, pela primeira vez, no ano de 2018, durante as festas juninas, as quais se constituem em um dos maiores eventos do país, mais conhecido como “O Maior São João do Mundo”.

Nos anos de 2018 e 2019, as empresas *Aliança Comunicação e Cultura e Medow Promo Serviços de Eventos e Estruturas Ltda.* – responsáveis pela organização desse evento, em parceria público/privada – trouxeram a tecnologia de reconhecimento facial para os festejos do “Maior São João do Mundo”, objetivando proporcionar maior segurança aos frequentadores da festa.

Embora, em 2018, os resultados não tenham sido os esperados, em 2019, a parceria entre *The Staff Solutions* – representante de uma companhia do Reino Unido,

desenvolvedora da plataforma digital *Facewatch* –, a Polícia Militar do Estado da Paraíba e um provedor de Internet local fez com que se concretizasse, de forma muito satisfatória, a implementação dessa tecnologia (DEMENTSHUK, 2019). Segundo este autor, foram instaladas 265 (duzentos e sessenta e cinco) câmeras de segurança, distribuídas em locais estratégicos do Parque do Povo, local de maior concentração dos festejos juninos da cidade e que possui 42.500 (quarenta e dois mil e quinhentos) metros quadrados de área.

A ação de reconhecimento facial de imagens dessas câmeras, empregada pela Polícia Militar, culminou na prisão de 11 (onze) pessoas, foragidas do sistema prisional ou com o mandado de prisão em aberto, durante o período das festividades. As abordagens aos possíveis suspeitos foram feitas pelo operador do sistema, no caso em comento, a Polícia Militar (BARBOSA, 2019).

A utilização de sistema de reconhecimento facial no “Maior São João do Mundo” foi considerada um sucesso: de acordo com o *site* oficial do Governo do Estado da Paraíba, na área do evento houve uma redução de 85% (oitenta e cinco por cento) dos incidentes registrados em 2019, pela Polícia Militar, quando comparados aos do ano de 2018.

Além disso, entrevistas levadas a efeito com frequentadores do evento, constataram que: (a) o monitoramento de segurança por câmeras recebeu a aprovação de 95,7% (noventa e cinco vírgula sete por cento) dos entrevistados; e (b) o evento foi considerado seguro para 60,7% (sessenta vírgula sete por cento) e extremamente seguro para 23,9% (vinte e três vírgula nove por cento) dos frequentadores entrevistados.

O governador do Estado da Paraíba, João Azevedo, afirmou que irá implementar projeto que prevê a instalação de 1.300 (mil e trezentas) câmeras nas cidades de João Pessoa, Campina Grande e Patos, bem como em pontos nas divisas com outros Estados, de forma a dispor de ampla gama de informações, desde a identificação de placas de veículos até o reconhecimento facial.

## **5 RISCOS DO USO DO RECONHECIMENTO FACIAL**

A ampliação da utilização da tecnologia de reconhecimento facial, ocorrida nos últimos anos, tem feito com que seja percebida, por vezes, como a solução para o problema da criminalidade. No entanto, diversos autores consideram que há, na

verdade, uma falsa sensação de segurança, desde que a ferramenta, além de ainda não ter uma eficiência comprovada, não está legalmente regulamentada. E essa normatização se torna mais necessária a partir do advento da Lei Geral de Proteção de Dados (Lei nº 13.709, de 14 de agosto de 2018), visto que dados biométricos passaram a ser considerados dados sensíveis, exceto para fins de segurança pública.

Segundo Lobato *et al.* (2020), o reconhecimento facial tem ganhado notoriedade junto a autoridades públicas, com aumento significativo dos casos de implantação por municípios e Estados do Brasil, entre os anos de 2018 e 2019. Para o autor, esse aumento é motivo de grande preocupação, visto que há poucas informações sobre como esta tecnologia está sendo implementada e testada, devido “à pouca transparência dos governos municipais e estaduais sobre os processos de aquisição, implementação e funcionamento do reconhecimento facial”.

Não sendo o objetivo deste artigo esgotar todos os debates acerca do tema proposto, há que se atentar para alguns problemas em relação à eficácia da tecnologia. Nesse contexto, um dos pontos mais importantes é que, como afirma Rodrigues (2019), os sistemas de reconhecimento facial apresentam resultados significativos quando as imagens analisadas são fotografias frontais, com boa iluminação e resolução. Todavia, continua ele:

[...] as taxas de acerto dos sistemas caem notoriamente em função de diversos fatores. Os erros aumentam quando são analisadas imagens com resolução baixa e provenientes de segmentos de vídeo, assim como devido a variações na iluminação, fundo da imagem, pose, expressão facial, sombras e distância da câmera.

O autor ainda complementa que, quanto maior o banco de dados, maior a probabilidade de falsos positivos – quando o sistema atribui, incorretamente, o rosto analisado a outro ao qual ele não corresponde de fato –, especialmente em minorias raciais e em mulheres, enfatizando que:

O viés é agravado no campo da segurança pública devido às relações históricas de desigualdade que conformam as condições de produção de muitas das bases de dados utilizadas. Portanto, populações socialmente vulneráveis poderiam ser sujeitas à automatização de constrangimentos e violências, como abordagens policiais indevidas e atribuição inverídica de antecedentes criminais.

Lobato *et al.* (2020) alertam que os sistemas de videomonitoramento, como o reconhecimento facial, utilizados em algumas cidades do Brasil, sofrem de algumas limitações, relacionadas: (a) com seu caráter técnico, quais sejam, a falta de pessoas

capacitadas para operar as câmeras e a escassez de recursos para investir na manutenção dos equipamentos; (b) com a perpetuação de injustiças e discriminações, através do uso da tecnologia; e (c) com a não solução do problema da insegurança nas cidades. Os autores enfatizam ainda que, até o momento, não foi identificado um estudo sistemático sobre a eficiência desses sistemas na prevenção e redução de delitos no país, nem há dados sobre os falsos positivos das implementações no país; assim, o sucesso que se tem apregoado para esses sistemas, baseia-se, exclusivamente, no critério de quantidade de prisões decorrentes de seu uso.

Na mesma linha de raciocínio, Varon (2019) argumenta que todos esses casos, no Brasil e em outros países que adotaram recentemente o uso de reconhecimento facial para fins de segurança pública, mostram que tanto há propensão a “abuso policial, como de abusos por parte do setor privado, tendo em vista que sua implementação envolve compartilhamento de dados sensíveis com as empresas privadas que implementam esses sistemas”.

Um ponto importante para reflexão é o fato de que, enquanto a utilização desses sistemas tende a ser cada vez mais estudada, melhorada e aplicada na segurança pública no Brasil, a cidade de São Francisco, nos Estados Unidos da América, foi a primeira “que decidiu proibir o uso do reconhecimento facial por sua polícia e a decisão foi baseada nos temores de que o uso abusivo da tecnologia compromettesse a privacidade dos cidadãos” (BERNARDO, 2019).

A privacidade e a imagem são direitos fundamentais invioláveis, conforme estabelece a Constituição Federal de 1988, em seu artigo 5º, inciso X: “são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação”. No entanto, esses direitos podem ser afetados, diante das formas de uso do reconhecimento facial. Neste aspecto Doneda (2011, p. 95) ressalta que:

Por meio da proteção de dados pessoais, garantias a princípio relacionadas à privacidade passam a ser vistas em uma ótica mais abrangente, pela qual outros interesses devem ser considerados, abrangendo as diversas formas de controle tornadas possíveis com a manipulação de dados pessoais. Para uma completa apreciação do problema, estes interesses devem ser considerados pelo operador do direito pelo que representam, e não somente pelo seu traço visível – a violação da privacidade.

Lobato *et al.* (2020) destacam que a privacidade é uma das principais discussões, no que se refere ao risco da utilização do reconhecimento facial, por se

constituir este em um mecanismo que realiza a captação de imagens, sem o conhecimento de quem tem a imagem de seu rosto analisada, bem como por empresas, em todo o mundo, terem construído bases de dados de rostos para realizar testes com tais sistemas; e acrescentam que:

(...) há o risco de essas bases serem comercializadas ou mesmo acessadas indevidamente por terceiros, se não forem armazenadas adequadamente ou se hackeadas. Além disso, outra preocupação que surge com o uso do reconhecimento facial é não se poder verificar a prática de coleta e o armazenamento das imagens captadas, devido à ausência de mecanismos de transparência adequados.

Lobato *et al.* (2020) também apontam que a falta de confiança nas instituições, pela falta de transparência com mecanismos que permitam avaliar, de modo independente, “a eficácia e o uso adequado do reconhecimento facial, assim como garantir o respeito à legislação de proteção de dados pessoais, gera incerteza sobre como esses sistemas são efetivamente utilizados”. E alertam quanto à importância de que o setor público seja transparente com a utilização desta ferramenta, de modo que a sociedade civil e a comunidade técnica “possam avaliar possíveis violações aos direitos humanos, se o investimento compensa, e colaborar com sugestões e mecanismos para se remediar erros e abusos”.

Neste diapasão, a pesquisadora em democracia e tecnologia Thayane Guimarães, do Instituto de Tecnologia e Sociedade do Rio de Janeiro (ITS), entrevistada por Marasciulo (2020), diz que o principal problema é a falta de uma legislação específica, que garanta as liberdades individuais, a transparência no uso da tecnologia de reconhecimento facial e a proteção de dados pessoais: a Lei Geral de Proteção de Dados Pessoais, em vigor desde 18 de agosto de 2020, não será aplicável ao tratamento de dados pessoais realizados para fins, exclusivamente, de segurança pública, defesa nacional, segurança do Estado; ou atividades de investigação e repressão de infrações penais, o que pode gerar abusos pelas autoridades para fins de monitoramento, o qual será regido por lei específica (ZAIDAN, 2019).

## **6 CONSIDERAÇÕES FINAIS**

O presente artigo não tem intenção de diminuir, desqualificar ou tender em sentido contrário no que concerne aos mecanismos que a segurança pública utiliza

para otimizar a prestação de serviços, mas sim de trazer a discussão para o polo passivo da utilização do sistema de reconhecimento facial: a sociedade.

Embora seja evidente que os sistemas de reconhecimento facial são uma tecnologia avançada, cuja utilização muito tem auxiliado a segurança pública no exercício de suas atribuições, é imprescindível que ocorra a disseminação de informação sobre essa utilização e seus impactos no cotidiano da sociedade.

Paralelamente, verifica-se que esses sistemas estão em constante desenvolvimento, possuindo falhas a serem corrigidas, de maneira a prevenir abusos em relação aos direitos individuais de cada um que é submetido à ferramenta. Embora tais correções exijam tempo, pesquisas e investimentos na área, é inegável que essa tecnologia já consegue trazer benefícios na otimização dos serviços públicos, principalmente na segurança pública, haja vista que o uso neste setor se destaca e possui números que comprovam a sua eficácia, a exemplo do “Maior São João do Mundo” no município de Campina Grande - Paraíba.

Há, portanto, um caminho extenso a se percorrer, para findar as questões sobre a utilização da ferramenta de reconhecimento facial, no que se refere aos indivíduos que são expostos a ela, fazendo-se necessário ampliar a percepção de que, sim, há responsabilidades éticas a serem tratadas no tocante às falhas do sistema.

Há, também, de se trazer para a pauta o início de regulações pelo Poder Legislativo, a fim de tornar essa utilização segura e eficiente para todos e definir, de forma firme e concreta, quem irá implementar, como e o que justifica seu uso, trazendo os princípios apontados pela Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709, de 14 de agosto de 2018), incentivando a fiscalização e estabelecendo as punições para os casos de abuso quanto aos dados coletados.

## REFERÊNCIAS

ALMEIDA, Alcides Ferreira. **Sistemas e tecnologias de informação para serviços policiais: o caso da Polícia Nacional de Cabo Verde**. 2009. Disponível em: <<http://bdigital.unipiaget.cv:8080/jspui/bitstream/10964/145/1/sistemas%20e%20tecnologias%20de%20inform%C3%A7ao.pdf>>. Acesso em: 01 dez. 2019.

BARBOSA, Hiran. “São João de Campina é o melhor caso de reconhecimento facial, batendo carnaval do Rio”, diz diretor da Staff. **Paraíba em Destaque**. Disponível em: <<https://www.paraibaemdestaque.com.br/2019/07/04/sao-joao-de-campina-e-o-melhor-caso-de-reconhecimento-facial-batendo-carnaval-do-rio-diz-diretor-da-staff/>>. Acesso em: 26 set. 2020

BATISTA, Gabriel de Almeida; NEVES, Felipe da Silva Borges; SANTOS, Igor Faggion Silveira; SCHINAID, Anderson Alves; SOUSA, Washington Lopes de. **Sistema de identificação e autenticação biométrica - Reconhecimento Facial**. São Paulo. (2017). Disponível em: <[https://www.academia.edu/35345642/Sistema\\_de\\_Identificacao\\_e\\_Autenticacao\\_Biometrica\\_Reconhecimento\\_Facial](https://www.academia.edu/35345642/Sistema_de_Identificacao_e_Autenticacao_Biometrica_Reconhecimento_Facial)>. Acesso em: 01 dez. 2019.

BERNARDO, Carlos Alberto Iglesia. **O reconhecimento facial e a LGPD**. Fundação Vanzolini Blog. (2019). Disponível em: <<https://vanzolini.org.br/weblog/2019/06/25/o-reconhecimento-facial-e-lgpd/>>. Acesso em: 25 set. 2020.

BRASIL. Constituição (1988). **Constituição**: República Federativa do Brasil. Brasília (DF): Senado Federal, 2015.

\_\_\_\_\_. Lei nº 13.709 de 14 de agosto de 2018. Lei Geral de Proteção e Dados. (LGPD). Redação dada pela Lei nº 13.853 de 2019. **Presidência da República**. Disponível em: <[http://www.planalto.gov.br/ccivil\\_03/\\_Ato2015-2018/2018/Lei/L13709.htm#ementa](http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm#ementa)>. Acesso em: 05 out. 2020.

DEMENTSHUK, Márcia Elisabeth. PARAÍBA. Governo do Estado da Paraíba. **PM usa inteligência artificial e ‘Internet das Coisas’ na PB**. (2019). Disponível em: <<https://paraiba.pb.gov.br/diretas/secretaria-da-educacao-e-da-ciencia-e-tecnologia/horizontes-da-inovacao/noticias/pm-usa-inteligencia-artificial-e-2018internet-das-coisas2019-na-pb>>. Acesso em: 30 set. 2020.

DONEDA, Danilo. (2011). A proteção dos dados pessoais como um direito fundamental. *Espaço Jurídico Journal of Law [EJLL]*, 12(2), 91-108. Disponível em: <<https://portalperiodicos.unoesc.edu.br/espacojuridico/article/view/1315>>. Acesso em: 15 ago. 2020.

FRANCISCO, Pedro Augusto P.; HUREL, Louise Marie; RIELLI, Mariana Marques. **Regulação de reconhecimento facial no setor público: avaliação de experiências internacionais**. 23 de junho de 2020. Instituto Igarapé. Disponível em: <<https://igarape.org.br/regulacao-do-reconhecimento-facial-no-setor-publico/>>. Acesso em: 23 ago. 2020.

GOMES, Dennis dos Santos. Inteligência Artificial: conceitos e aplicações. **Revista Olhar Científico**. Faculdades Associadas de Ariquemes. V. 01, nº 2, Ago/Dez 2010. Disponível em: <[https://www.academia.edu/28005380/Intelig%C3%Aancia\\_Artificial\\_Conceitos\\_e\\_Aplic%C3%A7%C3%B5es](https://www.academia.edu/28005380/Intelig%C3%Aancia_Artificial_Conceitos_e_Aplic%C3%A7%C3%B5es)>. Acesso em: 28 out. 2020.

HELOU, Rodolfo Miguel Soares. **Obrigação do estado em prestar segurança pública e sua responsabilidade quanto a sua desídia à luz da reserva do possível**. Brasília: EDIDP, 2008.

JUCÁ, Roberta Laene Costa. O papel da sociedade na política de segurança pública. **Revista Jus Navigandi**. Teresina, ano 7, nº 60, nov. 2002. Disponível em: <<https://jus.com.br/artigos/3525/o-papel-da-sociedade-na-politica-de-seguranca-publica/1>>. Acesso em: 30 nov. 2019.

LOBATO, Luisa Cruz; FRANCISCO, Pedro Augusto P.; HUREL, Louise Marie. **Mais câmeras, mais segurança?** Instituto Igarapé. (2020). Disponível em: <<https://igarape.org.br/videomonitoramento-webreport/#intro>>. Acesso em: 25 out. 2020.

LOHN, Josemar Müller. **Tecnologias aplicadas à segurança pública**. Palhoça Unisul Virtual. 2012. Disponível em: <<https://docplayer.com.br/4978042-Tecnologias-aplicadas-a-seguranca-publica.html>>. Acesso em: 28 nov. 2019.

MARASCIULO, Marília. Reconhecimento facial: prós e contras da tecnologia que veio para ficar. **Revista Galileu**. 22 Jun 2020. Disponível em: <<https://revistagalileu.globo.com/Tecnologia/noticia/2020/06/reconhecimento-facial-pros-e-contras-da-tecnologia-que-veio-para-ficar.html>>. Acesso em: 29 out. 2020.

NUNES, Fernanda Todesco. **Técnicas de biometria baseadas em padrões faciais e sua utilização na segurança pública**. Monografia submetida ao Programa de Pós-Graduação. Universidade Federal de Santa Catarina. Araranguá, 2015. Disponível em: <<http://150.162.242.35/handle/123456789/180402>>. Acesso em: 06 nov. 2019.

RODRIGUES, Gustavo. **Reconhecimento facial na segurança pública: Controvérsias, riscos e regulamentação**. Blog. Instituto de Referência em Internet e Sociedade, 27 de fevereiro de 2019. Disponível em: <<http://irisbh.com.br/reconhecimento-facial-na-seguranca-publicacontroversias-riscos-e-regulamentacao/>>. Acesso em: 15 nov. 2019.

SILVA, Alex Lima; CINTRA, Marcos Evandro. Reconhecimento de padrões faciais: Um estudo. **XII Encontro Nacional de Inteligência Artificial e Computacional (ENIAC)**. Natal. (2015). Disponível em: <[https://www.researchgate.net/publication/341625381\\_Reconhecimento\\_de\\_padroes\\_faciais\\_Um\\_estudo](https://www.researchgate.net/publication/341625381_Reconhecimento_de_padroes_faciais_Um_estudo)>. Acesso em: 26 out. 2020.

SILVA, Brigiane Machado da; VANDERLINDE, Marcos. **Inteligência artificial, aprendizado de máquina**. (2012). Disponível em: <[http://www.ceavi.udesc.br/arquivos/id\\_submenu/387/brigiane\\_machado\\_da\\_silva\\_\\_marcos\\_vanderlinde.pdf](http://www.ceavi.udesc.br/arquivos/id_submenu/387/brigiane_machado_da_silva__marcos_vanderlinde.pdf)>. Acesso em: 27 out. 2020.

SILVA, Victor Hugo. **Por que o uso de reconhecimento facial na segurança é controverso?** Blog. Tecnoblog, 7 de novembro de 2020. Disponível em: <<https://tecnoblog.net/380749/por-que-o-uso-de-reconhecimento-facial-na-seguranca-e-controverso/>>. Acesso em 16 nov. 2020.

VARON, Joana. Bem na sua cara: a ilusão do reconhecimento facial para segurança pública. **Coding Rights**. Disponível em: <<https://medium.com/codingrights/bem-na-sua-cara-a-ilus%C3%A3o-do-reconhecimento-facial-para-seguran%C3%A7a-p%C3%BAblica-47c708b34820>>. Acesso em: 27 set. 2020.

VIANA, Cleiton Correia; CONCEIÇÃO, Valdir Silva da; ROCHA, Angela Machado. Reconhecimento facial e a relativização do direito de imagem. Programa de Pós-Graduação em Propriedade Intelectual e Transferência de Tecnologia para a Inovação PROFNIT. Universidade Federal da Bahia (UFBA). Brasil. **Revista Ingi**. (2019). Vol. 3, n.3, p. 436-450. Jul/Ago/Set. — (Trimestral). Disponível em: <<http://ingi.api.org.br/index.php/INGI/article/view/50>>. Acesso em: 30 nov. 2019.

Z Aidan, Paula. **Proteção de dados impacta no uso de reconhecimento facial**. 04 de setembro de 2019. Disponível em: <<http://www.securityreport.com.br/destaques/protecaodedadosimpactanousodereconhecimentofacial/#.Xe4n4JNKjIW>>. Acesso em: 01 dez. 2019.