

ARTIGO

# Reconhecimento facial: entre a criminologia, a mídia e a LGPD penal

---

**Jéssica Guedes Santos**

[guedes.jessicas@gmail.com](mailto:guedes.jessicas@gmail.com)

Advogada no PG Advogados.  
Mestranda em Direito na  
Universidade de Brasília (UnB).

# Reconhecimento facial: entre a criminologia, a mídia e a LGPD penal

## **Palavras-chaves**

Reconhecimento facial  
segurança pública  
LGPD Penal  
Folha de São Paulo

## **Resumo**

O artigo tem como objeto o uso do reconhecimento facial para segurança pública no Brasil. A Lei Geral de Proteção de Dados (LGPD) apresenta parâmetros para a utilização de dados pessoais, inclusive pelo Poder Público. Todavia, a LGPD tem previsão específica determinando que lei específica trate sobre segurança pública, defesa nacional, segurança do Estado e atividades de investigação e repressão de infrações penais. Neste sentido, o anteprojeto sobre o tema foi entregue para a Câmara dos Deputados em novembro de 2020. A LGPD Penal pretende regular o tratamento de dados para fins de segurança pública e investigação penal, sendo que, dos arts. 42 ao 44, o anteprojeto trata do uso do reconhecimento facial para a segurança pública, questão que é vista com uma das vias para combate efetivo ao crime. Tendo como ponto de partida esta perspectiva legislativa, que dialoga com a privacidade e proteção de dados, o presente artigo analisa como a Folha de São Paulo aborda o tema nas suas reportagens de 2018 a 2020 com o intuito de investigar como a mídia analisa o uso do reconhecimento facial na segurança pública fazendo o cotejo entre tecnologia, mídia e criminologia. Foram encontrados três resultados principais, quais sejam, a cobertura sobre o tema no jornal ainda é incipiente; as manchetes têm problemáticas destacando as prisões realizadas com base na tecnologia, mas não abordam com eficácia a discriminação algorítmica e a perspectiva de privacidade e proteção de dados, mesmo que de forma genérica.

# Facial recognition: between criminology, media and brazilian general data protection law for public security

## Keywords

Facial recognition  
public security  
LGPD Penal  
Folha de São Paulo

## Abstract

The paper has as its subject the use of facial recognition in public security. Brazilian General Data Protection Law (LGPD) presents norms for the use of personal data by the individual or Government. However, the LGPD has a specific provision stipulating that another law deals with public security, national defense, state security and investigate activities and prosecution of criminal offenses. The project about the subject was submitted to the Parliament in November 2020. The project received the nickname LGPD Penal and deals with standards about the data processing for public security and investigative activities. The project deals about the use of facial recognition in public security in articles 42 to 44. Public opinion considers positive effectiveness of facial recognition to decrease the number of crimes. Thus, this paper raises how Folha de São Paulo – the newspaper with the largest circulation in Brazil – notices the subject from 2018 to 2020 in order to investigate how the media analyzes the use of facial recognition and public security. Three main results were found: the coverage is still incipient, the headlines have problems for being generic and exist the perspective of privacy and data protection even if in a generic way.

## 1. Introdução

O presente artigo busca analisar a interface entre tecnologia, criminologia e mídia com o recorte temático sobre o uso do reconhecimento facial para fins de segurança pública analisando os ditames da Lei Geral de Proteção de Dados Pessoais (LGPD) e do anteprojeto de Lei de Proteção de Dados para a segurança pública e a investigação criminal (LGPD Penal), e a forma que está sendo exposto pela mídia com o levantamento de notícias publicadas na Folha de São Paulo.

A LGPD foi publicada em 14 de agosto de 2018 e apresenta normas gerais sobre a proteção de dados no Brasil. Um dos impulsos para edição de um marco de proteção de dados no Brasil foi a série de escândalos que culminaram em violações de privacidade e uso indevido de dados pessoais. Porém, a vigência da Lei somente se iniciou em agosto de 2020.

Com a divulgação dos escândalos, a discussão acerca do uso da tecnologia como meio de controle foi amplificada e um dos aspectos que ganhou mais relevância foi o reconhecimento facial, especialmente por sua utilização na segurança pública em eventos e locais de grande movimentação. Todavia, também existe grande crítica sobre o uso dessa tecnologia pelas forças de segurança tanto pelo uso desenfreado que pode gerar uma vigilância em massa da população, como pelos aspectos preconceituosos resultantes da aplicação do reconhecimento facial (discriminação algorítmica).

Neste sentido, é interessante perceber como a imprensa faz a cobertura do tema diante do aspecto dúbio do reconhecimento facial: potencial benefício de uso para melhoria da vida em sociedade, mas possibilidade de violação constante de dados pessoais e de direitos fundamentais por meio da vigilância imotivada e propagação de preconceitos.

Segundo dados do Instituto Verificador de Comunicações (IVC, 2019), a Folha de São Paulo foi o jornal com maior circulação no Brasil em 2019, somando a circulação digital e impressa. Assim, o artigo pretende analisar de que forma a Folha de São Paulo tem realizado a cobertura do reconhecimento facial para a segurança pública partindo da hipótese que a cobertura do jornal pode influenciar a percepção pública sobre o tema. Para tanto, foi realizado levantamento no acervo do jornal constante de notícias de 14 de agosto de 2017 até 14 de dezembro de 2020, período escolhido por englobar um ano antes da edição da LGPD, a publicação da citada lei e o primeiro ano de sua vigência, permitindo analisar se a LGPD teve algum impacto nos termos da cobertura do jornal sobre o assunto.

Este recorte foi realizado diante da importância da LGPD no campo da privacidade e proteção de dados no país, já que é a principal norma da temática. Apesar do Marco Civil da Internet (MCI) elencar a privacidade como um dos princípios da internet, não aborda o tema de forma aprofundada como faz a LGPD. Além do aspecto normativo, a LGPD pretende fomentar os aspectos culturais e organizacionais da privacidade e proteção de dados, perspectivas que devem influenciar em toda a sociedade, inclusive no uso de tecnologias pelo Estado. Assim, o levantamento das reportagens indicará se houve mudança na forma que o jornal trata o tema após a publicação da LGPD.

O artigo é dividido em três partes. A primeira trata sobre a importância da proteção de dados no país avaliando os aspectos da LGPD e da chamada LGPD Penal no que diz respeito ao reconhecimento facial e sua potencial utilização na segurança pública. A segunda apresenta o resultado da coleta documental do acervo da Folha. A terceira faz o cotejo entre o exposto pela legislação, o informado pelo jornal e as considerações necessária realizadas pela criminologia.

## 2. A Proteção de Dados no Brasil e o Reconhecimento Facial

O conceito jurídico de privacidade só surgiu em 1890 com o artigo *The Right to Privacy* de Louis D. Brandeis e Samuel D. Warren (1890) e, na época, a privacidade tinha um contexto negativo, que pretendia firmar uma ideia de isolamento, de tranquilidade, de ser deixado só.

Porém, com o passar do tempo, o conceito jurídico de privacidade foi alterado diante de importantes mudanças sociais como o estado de bem-estar social, a luta por mais direitos pelos movimentos sociais, o aumento do fluxo de informações e o desenvolvimento tecnológico (DONEDA, 2019). A privacidade passou a abarcar características fundamentais para o desenvolvimento e livre exercício do direito de personalidade, e ainda “tem importância para uma sociedade democrática como pré-requisito fundamental para o exercício de diversas outras liberdades fundamentais” (DONEDA, 2019, p.31).

Decorrente do direito à privacidade, anos depois, em 1970, surge a proteção de dados pessoais por conta da importância que a informação pessoal - relacionada as informações referentes a características da pessoa – ganhou tanto no âmbito público com a formação de políticas públicas quanto no privado no âmbito comercial (DONEDA, 2011). A proteção de dados busca garantir que o cidadão seja o centro da relação de troca das suas informações pessoais com o Estado e com a iniciativa privada permitindo que ele tenha plena ciência de quando, como e por qual motivo as suas informações são utilizadas (DONEDA, 2011).

Assim, a privacidade surge com contornos jurídicos relacionados à defesa de características manifestas dos indivíduos garantindo ao mesmo tempo a não intervenção indevida e a esfera de abrigo para o exercício de demais

direitos fundantes da personalidade. Já a proteção de dados, mesmo vinculada à privacidade, tem um aspecto diferente e assumiu perspectivas próprias buscando garantir individual e coletivamente “a efetiva tutela da pessoa em vista de variadas formas de controle e contra a discriminação, com o fim de garantir a integridade de aspectos fundamentais de sua própria liberdade pessoal.” (DONEDA, 2019).

Observa-se que desde o início dos anos 2000 a tecnologia passou por uma crescente mediante a popularização da internet e de aparelhos que permitem a sua conexão. Neste sentido, importante mencionar que a pesquisa TIC Domicílios 2019 publicada em novembro de 2020 e anualmente realizada pelo Comitê Gestor da Internet (CGI.br) aponta que 71% (setenta e um por cento) do total dos domicílios brasileiros tem acesso à internet e cerca de 134 (cento e trinta e quatro) milhões de brasileiros são usuários da internet.

O desenvolvimento da internet também atingiu o Poder Público. Atualmente, segundo dados do site do Governo Digital, mil serviços públicos foram digitalizados em menos de dois anos e a Estratégia de Governo Digital de 2020 a 2022 (Decreto nº 10332/2020) prevê como objetivos como a oferta de serviços públicos digitais, a avaliação de satisfação nos serviços digitais e o acesso digital único aos serviços públicos. Neste sentido, a tecnologia passou a ser aplicada em vários setores pelo Poder Público, inclusive na segurança pública. Por isso, é necessário refletir acerca dos aspectos da proteção de dados no país buscando garantir a transparência (FRAZÃO, 2020).

Assim, a governança da internet, que é área que se encarrega de estudar os aspectos técnicos-regulatórios necessários para o funcionamento e desenvolvimento da internet (KURBALIJA, 2016), já apontava a importância de se pensar em formas legais e/ou regulatórias de proteção dos usuários da rede ao menos desde a Cúpula Mundial sobre a Sociedade da

Informação em 2003<sup>1</sup>. Todas essas discussões se intensificam após 2013 com a divulgação por Edward Snowden de um sistema de espionagem feito pela Agência de Segurança Nacional (NSA) dos Estados Unidos para vigiar cidadãos estadunidenses e de outros países.

No Brasil, a primeira legislação voltada exclusivamente para o âmbito virtual surgiu logo após o caso Snowden, com a publicação do Marco Civil da Internet (MCI), Lei Federal nº 12965/2014<sup>2</sup>. O MCI estabelece princípios, garantias, direitos e deveres para o uso da internet no país e, no que diz respeito ao objeto deste artigo, o MCI aponta como princípios a proteção da privacidade e a proteção dos dados pessoais na forma da lei no art. 3º, II e III<sup>3</sup>, respectivamente.

Mas, apesar de ser ponto importante do MCI por compor a base principiológica da Lei, a proteção de dados não foi tratada em detalhes pelo MCI. Inclusive, a própria disposição acima citada aponta a necessidade de uma lei específica para tratar sobre o assunto. E, depois de alguns anos de discussão no Legislativo Federal, a Lei foi publicada. A Lei Geral de Proteção de Dados Pessoais (LGPD), Lei Federal nº 13709/2018, foi publicada em 14 de agosto de 2018 com vigência iniciada no final de agosto de 2020.

Com a LGPD, o Brasil passa a ter parâmetros legais para a proteção de dados, que também abarca o reconhecimento facial. Os dados genéticos, biométricos e de saúde são considerados dados pessoais sensíveis<sup>4</sup>, o que significa dizer que são informações muito importantes porque conseguem identificar aspectos únicos de uma pessoa com possibilidade de uso para fins discriminatórios. Por isso, a LGPD estipula critérios específicos para o tratamento<sup>5</sup> desses dados, como o consentimento específico e destacado para finalidades específicas informadas pelo agente de tratamento de dados.

A tecnologia de reconhecimento facial precisa se utilizar de dados da face para conseguir rodar o algoritmo e identificar uma pessoa, portanto, o reconhecimento facial parte do uso de dados

biométricos, que são considerados dados pessoais sensíveis nos termos do art. 5º, II da LGPD<sup>6</sup>.

Basicamente, o reconhecimento facial funciona com a seguinte metodologia: a inteligência artificial é treinada por meio de um banco de dados com várias imagens para extrair características específicas (como a distância do nariz aos olhos, da boca ao queixo, o formato do rosto, etc) e assim consegue identificar características biométricas das faces com base em padrões definidos. Depois de pronto, a ideia é que o algoritmo consiga reconhecer e identificar um rosto com uma foto ou um vídeo (SILVA, 2021).

Neste sentido, a pesquisadora Joy Buolamini (2016) expôs os problemas do preconceito algorítmico, que perpetua a discriminação e a exclusão de direitos, por meio de um experimento com um software genérico de reconhecimento facial: o algoritmo não reconhecia o seu rosto - a pesquisadora é negra - mas, quando ela colocava uma máscara branca, o software reconhecia que uma pessoa estava ali. Esse problema acontecia por conta da forma que é feito o treinamento da *machine learning*. Como expõe a pesquisadora:

a visão informática usa técnicas de aprendizagem de máquinas para fazer o reconhecimento facial. Funciona assim: criamos um grupo de formação com exemplos de rosto. Isto é um rosto, isto não é um rosto. Com o tempo, podemos ensinar o computador a reconhecer rostos. Contudo, se os grupos de formação não forem diversificados, qualquer rosto que se desvie demasiado da norma estabelecida será difícil de detectar. Foi o que aconteceu comigo (BUOLAMINI, 2016).

Ou seja, o uso desenfreado do reconhecimento facial, em um momento no qual a maioria das empresas ainda não tem times diversos<sup>7</sup> e nem a privacidade como padrão para impedir

violação da privacidade e da proteção de dados, culmina no racismo algoritmo manifestado de duas formas: no desenvolvimento do algoritmo com invisibilidade de critérios físicos fora do padrão estabelecido e na aplicação da tecnologia com os efeitos de manutenção de preconceitos pelos vieses algorítmicos que geram desumanização e invisibilidade (SILVA, 2020).

Todavia, por conta da lógica de identificação praticamente instantânea, o reconhecimento facial tende a se expandir em setores que buscam o monitoramento. Levantamento feito pelo Instituto Igarapé (2019) demonstra que desde 2011 foram encontrados 48 (quarenta e oito) casos reportados publicamente de implementação de reconhecimento facial no Brasil pelo Poder Público ou parceiros no setor privado nas áreas de educação, transporte, controle de fronteiras e segurança pública. As principais áreas na temática são o transporte e a segurança pública, com 21 (vinte e um) e 13 (treze) projetos de implementação, respectivamente.

Assim, existe uma nítida relação entre os dados pessoais sensíveis, a proteção de dados e a segurança pública no que diz respeito ao reconhecimento facial. Porém, a LGPD não trata sobre o assunto, uma vez que o art. 4º, III estabelece que a Lei não se aplica para fins exclusivos de segurança pública, defesa nacional, segurança do Estado e atividades de investigação e repressão de infrações penais. No entanto, a própria LGPD estabelece no art. 4º, §1º que esses temas devem ser tratados por uma lei específica<sup>8</sup>.

Neste sentido, foi designada uma comissão de juristas pelo presidente da Câmara dos Deputados para redigir um anteprojeto sobre o tema em novembro de 2019<sup>9</sup>. A Comissão entregou o anteprojeto para a Câmara no começo de novembro de 2020. O anteprojeto ainda deve ser distribuído e passar por todo o trâmite na Câmara dos Deputados e no Senado Federal para depois ser publicado e transformado em legislação, porém, analisar o anteprojeto é importante para verificar as premissas que foram

fixadas neste primeiro projeto de lei sobre o uso de dados para a segurança pública e as possíveis normatizações que podem ser relacionadas com o reconhecimento facial.

Assim, a chamada LGPD Penal busca apresentar normas gerais sobre o tratamento de dados para fins de segurança pública e investigação penal por meio dos seus 12 (doze) capítulos divididos em 68 (sessenta e oito) artigos<sup>10</sup>. O capítulo VII, que compreende os arts. 42 – 44, foi intitulado de “tecnologias de monitoramento e tratamento de dados de elevado risco” e, portanto, engloba o uso do reconhecimento facial para a segurança pública.

Nos termos dos supracitados artigos, a utilização de tecnologias de monitoramento devem ser previstas por lei específica que autorize a sua utilização elencando os direitos dos titulares e fundamentadas em relatório de impacto de vigilância, sendo que, o relatório de vigilância mencionado deve ser composto por uma avaliação de risco da atividade englobando a descrição da natureza dos dados envolvidos, as finalidades específicas do tratamento e a quantidade de titulares de dados potencialmente atingidos, entre outros aspectos. Inclusive, a lei específica deve ser acompanhada de uma avaliação de impacto regulatório<sup>11</sup>.

A LGPD Penal estabelece que o Conselho Nacional de Justiça (CNJ) emita recomendações sobre o uso dessas tecnologias, inclusive o CNJ deve publicar relatório anual sobre o uso de tecnologias de monitoramento pelas autoridades e realizar auditoria diante de denúncia de descumprimento da legislação. Assim, segundo a proposta do anteprojeto, o reconhecimento facial utilizado para fins de segurança pública deve ser previsto em lei específica para tal e com a apresentação de relatório de impacto de vigilância, sendo que, o CNJ faz o controle do uso desta tecnologia<sup>12</sup>.

Mas, para além disso, o anteprojeto ainda estabelece uma questão fundamental no art. 43 quando expõe que

Art. 43 - No âmbito de atividades de segurança pública, é vedada a utilização de tecnologias de vigilância diretamente acrescida de técnicas de identificação de pessoas indeterminadas em tempo real e de forma contínua quando não houver a conexão com a atividade de persecução penal individualizada e autorizada por lei e decisão judicial.

Ou seja, o reconhecimento facial não poderia estar em funcionamento em período integral e de forma genérica, já que a citada disposição aponta que a vigilância na segurança pública deve ser feita de forma individualizada autorizada pela lei e por decisão judicial<sup>13</sup>.

### 3. As Reportagens da Folha de São Paulo

#### 3.1. Metodologia

O tópico acima apresentou um panorama sobre a proteção de dados e o monitoramento realizado por meio do reconhecimento facial na segurança pública com base nas premissas da LGPD e das ideias presentes no anteprojeto da LGPD Penal. Neste tópico iremos apresentar como a mídia trata do assunto selecionando reportagens da Folha de São Paulo, jornal com maior tiragem física e digital do país em 2019 (IVC, 2019), para em seguida fazer a análise do exposto pelo jornal.

O levantamento do acervo foi realizado nos períodos de 14 de agosto de 2017 a 14 de dezembro de 2020, período escolhido por englobar o ano antes da edição da LGPD (ago/2017 a jul/2018), a publicação e a vigência da Lei (ago/2018 a ago/2020) e a apresentação do

anteprojeto da LGPD Penal (nov/2020) e, portanto, permite averiguar se existe alguma mudança de posicionamento da divulgação das notícias pelo jornal após a edição do marco legal de proteção de dados no país.

A coleta de dados foi realizada por meio do acervo *online* da Folha de S. Paulo<sup>14</sup> na Edição Folha, que corresponde a versão diária impressa e online do jornal. O site tem dois padrões de busca: um para as edições de até 6 (seis meses) meses atrás e outro para as demais edições. Como a presente pesquisa engloba um período de 40 (quarenta) meses foi preciso utilizar os dois padrões ter acesso aos dados apresentados, sendo que o filtro de busca avançado utilizado foi a expressão “reconhecimento facial”.

#### 3.2. Reportagens do ano anterior a publicação da LGPD

No período de 14 de agosto de 2017 a 13 de agosto de 2018 (ano anterior a publicação da LGPD) foram encontrados 31 (trinta e um) resultados<sup>15</sup>, sendo que 3 (três) trataram especificamente sobre segurança pública<sup>16</sup>:

1. Coluna de opinião, 31 de outubro de 2017: a coluna foi escrita por Eduardo Navarro, então presidente da Telefônica Brasil. Intitulada de “Depois do Digital”, sem maiores considerações, a coluna expõe que “as cidades inteligentes serão mais seguras com câmeras de reconhecimento facial, terão energia limpa e transporte mais eficiente. Viveremos melhor<sup>17</sup>.”

2. Reportagem, 08 de abril de 2018<sup>18</sup>: escrita por Filipe Oliveira sob o título “Fim do anonimato”, a reportagem apresenta uma série de considerações sobre o uso do reconhecimento facial para diversos fins. Sobre o uso de dados biométricos faciais pela Polícia, o jornalista aponta que o risco de uso indevido está



presente no mundo todo e cita estudo fundamentando o desvirtuamento do uso para coibição de manifestações políticas ao invés do suposto dever de proteção da população.

3. Reportagem, 01 de maio de 2018<sup>19</sup>: Alvaro Costa e Silva apresenta caso de reconhecimento facial na China no qual suspeito de crime financeiro foi identificado pelo algoritmo quando entregava ingresso para entrar em um evento esportivo e faz críticas ao uso indevido da tecnologia na segurança pública.

### 3.3. Reportagens do ano da publicação da LGPD

No período de 14 de agosto de 2018 a 13 de agosto de 2019 (ano de publicação da LGPD) foram encontrados 42 (quarenta e dois resultados)<sup>20</sup>, sendo que 2 (dois) sobre segurança pública<sup>21</sup>:

I. Artigo de opinião, 11 de setembro de 2019<sup>22</sup>: foi escrito por Hannah Fry, professora de matemática da University College London. No texto, a professora expõe caso ocorrido em festival na Inglaterra no qual a polícia aplicou reconhecimento facial para buscar 500 (quinhentas) pessoas que seriam alvos de prisão. Mas, no final, foram presas 96 (noventa e seis) pelo uso do algoritmo, sendo que somente uma seria alvo de mandado de prisão, todas as outras foram prisões equivocadas. Assim, o título do artigo aponta o fundamento central do texto: “não acredite cegamente em algoritmos porque até eles erram.”

2. Reportagem, 17 de julho de 2019<sup>23</sup>: foi escrita por Fabrício Lobel com o título “Metrô de São Paulo terá sistema de vigilância com reconhecimento facial” apontando o crescimento do parque de câmeras do metrô para 5.200 (cinco mil e duzentos) aparelhos nos próximos três anos. Para a reportagem, o presidente do Metrô/SP apontou que “esse projeto, do jeito que está,

não está vinculado à Secretaria de Segurança Pública. Mas ele permite que possa ser feito um convênio com a secretaria, receber o banco de dados deles e que utilizemos para monitorar o Metrô”. A reportagem cita uso semelhante nos estados da Bahia e do Rio de Janeiro destacando que a utilização pode ter problemas, como a identificação errada de pessoas, a vigilância excessiva e a repressão de minorias.

### 3.4. Reportagens do ano de vigência da LGPD e da apresentação da LGPD Penal

No período de 14 de agosto de 2019 a 14 de dezembro de 2020 (ano de vigência da LGPD e apresentação do anteprojeto da LGPD Penal) foram encontrados 69 (sessenta e nove resultados)<sup>24</sup>, e 8 (oito) deles tratam sobre segurança pública<sup>25</sup>:

I. Reportagem, 19 de outubro de 2019<sup>26</sup>: escrita por Luís Francisco Carvalho Filho e aponta o uso de reconhecimento facial no carnaval de Salvador e do Rio de Janeiro apontando que é preciso estar atento aos erros e a vigilância estimulada pela inteligência artificial.

2. Reportagem, 24 de outubro de 2019<sup>27</sup>: e não tem indicação de autoria, mas faz parte do caderno especial “Foco nos Estados: Bahia”. A reportagem nomeada de “Tecnologia e integração no combate à criminalidade: cai número de homicídios com novas ferramentas e aproximação das forças de segurança” apresenta que o uso do reconhecimento facial para a segurança pública no estado é um sucesso, pois “implantada no início do ano, a nova tecnologia já ajudou a capturar mais de 60 pessoas procuradas pela polícia – um dos flagrados pelo sistema estava fantasiado de mulher e brincava em um bloco de Carnaval.”

3. Reportagem, 23 de novembro de 2019<sup>28</sup>: escrita por Júlia Borbon com o título “reconhecimento facial já levou a 151 prisões no país.” A reportagem apresenta os dados do relatório da Rede de Observatórios da Segurança, que fez pesquisa sobre o número de pessoas presas por reconhecimento facial no país levantando ainda episódios de racismo, operações policiais e chacinhas. A reportagem ainda destaca que “não há, porém, diz o relatório, preocupação dos governos em elaborar protocolos para proteger esses dados, ignorando a Lei Geral de Proteção de Dados Pessoais, sancionada no ano passado.”

4. Reportagem, 29 de janeiro de 2020<sup>29</sup>: foi escrita por Thaiza Pauluze e aponta em nota o uso do reconhecimento facial no carnaval de São Paulo pela Polícia apresentando o sistema sem maiores detalhamentos.

5. Reportagem, 18 de fevereiro de 2020<sup>30</sup>: de título “fim de semana pré-Carnaval tem 413 detidos em SP” não tem autoria mencionada e também trata sobre o uso do reconhecimento facial no carnaval de São Paulo apontando apenas que “a tecnologia de reconhecimento facial a partir de imagens de câmeras da polícia também foi usada nos desfiles e ajudou a localizar e prender as pessoas foragidas”.

6. Reportagem, 20 de fevereiro de 2020<sup>31</sup>: foi publicada no “Caderno Especial: Inteligência Artificial” sem a indicação de autoria. Sob o título “Reconhecimento facial salva vidas, mas cerceia liberdades: sistema que ajuda a segurança pública esbarra na invasão da privacidade”, a matéria aponta a possibilidade de uso benefício da tecnologia – como no caso de busca de crianças e pessoas desaparecidas –, porém aponta o risco da vigilância exacerbada e dos vieses elencando que “um estudo do governo americano aponta que o reconhecimento facial tem dificuldade para identificar negros e asiáticos.”

7. Opinião, 23 de fevereiro de 2020<sup>32</sup>: escrita por Robert Muggah e Pedro Augusto P. Francisco. O próprio título e resumo expõe o

defendido no texto: “Polícia do futuro, riscos de sempre: Novas tecnologias de combate ao crime proliferam no Brasil como promessa de eficiência, contudo ferramentas de reconhecimento facial e de previsão de delitos podem minar liberdades civis e estimular discriminação se mal administradas.”

8. Coluna, 14 de setembro de 2020: nota publicada na coluna da Mônica Bergamo com os seguintes ditames: “De olho – Segundo levantamento do grupo [AqualtuneLab], 184 pessoas foram presas em 2019 com uso de reconhecimento facial em seis estados brasileiros. Dos casos sobre os quais há informações, 90,6% dessas pessoas eram negras<sup>33</sup>.”

### 3.5. Resultados encontrados no jornal

Assim, nos 40 (quarenta) meses investigados foram encontradas 13 (treze) reportagem/opiniões na Folha de São Paulo acerca do uso do reconhecimento facial para a segurança pública. Observa-se que o número de menções gerais ao reconhecimento facial nas publicações do jornal subiu bastante ao longo do período pesquisado: 2017/2018 – 31 (trinta e um); 2018/2019 – 42 (quarenta e dois) e 2019/2020 – 69 (sessenta e nove), o que demonstra a importância do tema.

Com relação ao que foi encontrado sobre o reconhecimento facial na segurança pública, dois textos (Coluna de opinião, 31 de outubro de 2017 e Reportagem, 24 de outubro de 2019) têm uma perspectiva de que o reconhecimento facial possui papel primordial na segurança pública, e de que afastá-lo desse uso seria prejudicial para a sociedade.

Todavia, os demais textos não deixam de destacar a importância que esta tecnologia pode ter para o combate de crimes, mas também

apontam com precisão os problemas que envolvem seu uso nesta esfera e que não podem ser ignorados: a identificação errada, o viés discriminatório, a vigilância em massa, a violação da proteção de dados e violação da LGPD, o uso irregular dessa tecnologia pela polícia, a ausência de parâmetros legais e a violação da privacidade.

#### **4. O Reconhecimento Facial, a Proteção de Dados, a Mídia e o Crime**

Sobre o objeto do artigo, é importante ressaltar que o uso amplo e sem regulação do reconhecimento facial tende a perpetrar uma série de violações de direitos, especialmente de grupos minoritários. A aplicação do reconhecimento facial na segurança pública encontra os mesmos problemas, que ainda são agravados por lidar com a persecução penal e criminologia. Como extraído das reportagens identificadas no tópico anterior, apesar das críticas formuladas, existe uma perspectiva que o reconhecimento facial é um grande aliado das forças policiais e que seria a forma de acabar e/ou diminuir consideravelmente a criminalidade.

Porém, esses vieses do algoritmo trazem grandes problemas para o campo criminológico relacionado a perpetuação de discriminação de minorias. Interessante menção destacada da coluna de Mônica Bergamo de 14 de setembro de 2020 aponta que 90,6% das pessoas presas via reconhecimento facial em 2019 eram negras. A coluna divulga o estudo da Rede de Observatórios da Segurança que apontou i) a dificuldade de saber como as prisões foram feitas e quantas prisões foram equivocadas, mesmo utilizando a Lei de Acesso à Informação; ii) o uso em 42,2% para prisões relacionados ao tráfico de drogas e roubo e iii) a baixa efetividade do sistema (NUNES, 2019).

Como aponta uma das reportagens levantadas que trata sobre o viés algorítmico do reconhecimento facial, em 2019, o software de reconhecimento da Amazon confundiu 27 (vinte e sete) atletas com criminosos<sup>34</sup>. A reportagem não explora os motivos pelos quais os atletas teriam sido confundidos pelo algoritmo, mas não é novidade que o reconhecimento facial é evado de erros desta dimensão conhecidos como vieses algorítmicos.

Pablo Nunes (2021), coordenador do Centro de Estudos de Segurança e Cidadania (CESeC) ainda aponta que os projetos relacionados ao uso do reconhecimento facial na segurança avançaram no Brasil sem maiores resistências – e o levantamento das reportagens realmente demonstra um número baixo de menções ao tema, o que indica, ao menos, que o maior jornal do país não tem muito apego pelo assunto – e que temos um problema prévio à tecnologia:

E mesmo que o Brasil já tivesse uma LGPD Penal, que as recomendações internacionais fossem seguidas, que os algoritmos tivessem 100% de acerto, ainda assim teríamos um problema que é anterior a qualquer tecnologia. Hoje o Brasil tem 773.151 pessoas cumprindo pena de privação de liberdade, uma taxa de crescimento da população carcerária entre as maiores do mundo; essas pessoas, a maioria negras, estão presas em grande parte por crimes sem violência. E por mais que o número de presos cresça a cada ano, não vemos redução da criminalidade. Nesse cenário bem conhecido, os proponentes do uso de reconhecimento facial pela polícia parecem estar esperando resultados distintos, mas apostam em acelerar ainda mais o encarceramento, a mesma lógica que tem guiado a segurança pública em todos esses anos.

Assim, o reconhecimento facial continua transmitindo a imagem parcial da criminalidade relacionado com o aspecto que Alessandro Baratta (1994) chamou de criminalidade tradicional, que somente recai sobre os crimes realizados pelas classes sociais menos abastadas, como furto e roubo, e acaba sendo relacionado ao “estereótipo do criminoso”. Como citado, no levantamento feito pela Rede de Observatórios da Segurança, o roubo foi um dos crimes que mais movimentou o uso do reconhecimento facial do país e mais de 90% das pessoas presas com o uso dessa tecnologia foram identificadas como negras.

Da mesma forma que a pesquisa realizada pelo professor Alessandro Baratta (2014, p.16) na Alemanha concluiu que “é grande diferença entre o sentimento genérico de temor do perigo criminal e a percepção de probabilidade efetiva de ser vitimizado no próprio bairro e na própria casa. O sentimento genérico de medo é desproporcionalmente maior que o medo de tornar-se concretamente objeto de uma ação criminal”, observa-se que o uso do reconhecimento facial na segurança pública também consiste em medida potencialmente ineficaz que visa fornecer uma falsa sensação de segurança, já que os dados do levantamento demonstram que a captura do rosto de 1,3 milhões de pessoas geraram 903 (novecentos e três) alertas e somente 33 (trinta e três) tinham real fundamento. Portanto, no estado da Bahia em 2019 tivemos o pífio índice de 4% (quatro por cento) de correspondência entre alertas e mandados (NUNES, 2019).

Ademais, é equivocado afirmar como aponta de forma genérica a coluna de opinião de 31 de outubro de 2017 que o reconhecimento facial gera mais segurança e acabar com o crime. “O crime é um fenômeno resultante da forma como administramos a convivência social, como nós construímos a cidadania e as relações sociais (CERQUEIRA, 1994, p. 34)” e não é aplicação do reconhecimento facial que vai mudar

esses aspectos tão latentes da nossa sociedade.

A mídia pode contribuir para fomentar essas visões equivocadas acerca do reconhecimento facial na opinião pública, especialmente se focar somente no aspecto da prisão (CERQUEIRA, 1994)<sup>35</sup>. Não se olvida que a mídia pode incitar o “populismo punitivo” inflamando a “opinião publicada” para que busque a ampliação do uso desta tecnologia na segurança pública vendendo-a como solução para a criminalidade (BARATA, 2008), até mesmo pela cultura midiática do delito desde o surgimento dos meios de comunicação em massa (BARATA, 2003).

Diante destes fatos, a Folha de São Paulo parece ter uma visão moderada sobre o assunto no período estudado apontando a crescente do reconhecimento facial como forma de melhorar a segurança pública. Mas, na ampla maioria das notícias, são expostos os problemas inerentes à vigilância extrema, o que se encaminha de forma diversa da hipótese fixada que avaliava que as notícias teriam uma postura mais favorável ao reconhecimento facial.

Porém, é preciso destacar quatro aspectos que chamaram atenção ao longo do estudo: (i) várias das notícias destacadas tem manchetes relacionadas à prisão de indivíduos, mesmo que no corpo do texto se tenha o contraponto ao uso da tecnologia; (ii) a maioria das notícias trata em alguma medida da problemática entre reconhecimento facial, proteção de dados e privacidade; (iii) o jornal tratou poucas vezes sobre o tema no período pesquisado; (iv) apesar da maioria das notícias coletadas indicar as críticas mais realizadas ao reconhecimento facial na segurança pública pelos estudiosos do tema, nenhuma delas tratou de forma aprofundada o problema da perpetuação da discriminação pelo reconhecimento facial.

## 5. Conclusão

O presente artigo analisou a interconexão entre tecnologia, mídia e criminologia abordando como a Folha de São Paulo fez a cobertura do uso do reconhecimento facial na segurança pública no período de 14 de agosto de 2017 a 14 de dezembro de 2020.

Como o reconhecimento facial envolve necessariamente o uso de dados com a identificação da face foi preciso explorar como a LGPD e o recente anteprojeto da LGPD Penal tratam sobre o assunto para verificar se existe algum tipo de conexão entre o discurso midiático, à privacidade e à proteção de dados e o reconhecimento facial.

Portanto, a primeira parte do artigo tratou sobre a proteção de dados no Brasil e o reconhecimento facial apontando que os dados biométricos são dados pessoais sensíveis pela LGPD e que devem ser utilizados nos termos previstos pela Lei para evitar violação à privacidade e garantir a proteção desses dados. Também foram analisados os arts. 42 - 44 da LGPD Penal que tratam sobre tecnologias de monitoramento e tratamento de dados de elevado risco a fim de identificar os possíveis critérios legais para o uso do reconhecimento facial na segurança pública no país, com o destaque para previsão do anteprojeto que impede o uso integral e genérico e elenca o Conselho Nacional de Justiça como autoridade central de fiscalização do tema.

A segunda parte do artigo consistiu no levantamento das reportagens da Folha de São Paulo, no qual culminou no total em 142 (cento e quarenta e dois) menções ao termo reconhecimento facial no geral, sendo que somente 13 (treze) opiniões e/ou reportagens trataram especificamente de algum ponto sobre o reconhecimento facial na segurança pública. 2 (dois) dos artigos encontrados defendem que o reconhecimento facial deve ser utilizado sem maiores

temores para a segurança pública, mas os demais apontam que a questão também envolve problemas sérios, como a vigilância em massa e o uso abusivo dos dados dos cidadãos.

A terceira parte do artigo faz o cotejo entre os dados encontrados com a criminologia apontando que o reconhecimento facial na segurança pública tende a contribuir para violações de direitos, especialmente de grupos minoritários. Foi destacada a necessidade da privacidade como padrão (privacy by design) e a diversidade dos times de desenvolvedores para fomentar um melhor desempenho da tecnologia. O algoritmo é treinado para seguir os padrões presentes no seu banco de dados e, na maioria das vezes, é afetado de vieses que são percebidos na sua aplicação diante de consequências preconceituosas, como a mencionada por Joy Buolamini. Assim, o reconhecimento facial na segurança apresenta problemas que foram destacados por reportagens no jornal, como a baixa efetividade e a discriminação contradizendo assim a hipótese inicial.

Por fim, percebe-se que a cobertura da Folha de São Paulo sobre o tema ainda é incipiente, já que das 142 (cento e quarenta e duas) menções encontradas, somente 13 (treze) enfrentaram o tema diretamente. Mas foi possível extrair alguns aspectos da cobertura sobre o reconhecimento facial e a segurança pública: problemáticas nas manchetes que destacam somente o aspecto de prisão quando trata de reconhecimento facial; a perspectiva da privacidade e da proteção de dados se faz presente quando o assunto é tratado, mesmo que seja de forma genérica e a falta de necessária exposição das formas como o reconhecimento facial fomenta a discriminação, ou seja, reportagens mais abrangentes sobre o uso do reconhecimento facial na segurança pública.

## Referências

- Acervo da Folha de São Paulo. Acesso em 09 de janeiro de 2021. Disponível em: <https://acervo.folha.com.br/index.do>.
- Anteprojeto da Lei de Proteção de Dados para segurança e persecução penal. Acesso em 03 de janeiro de 2021. Disponível em: [https://www2.camara.leg.br/atividade-legislativa/comissoes/grupos-de-trabalho/56a-legislatura/comissao-de-juristas-dados-pessoais-seguranca-publica/documentos/outros\\_documentos/DADOSAnteprojetoComissaoProtecaoDadosSegurancaPersecucaoFINAL.pdf](https://www2.camara.leg.br/atividade-legislativa/comissoes/grupos-de-trabalho/56a-legislatura/comissao-de-juristas-dados-pessoais-seguranca-publica/documentos/outros_documentos/DADOSAnteprojetoComissaoProtecaoDadosSegurancaPersecucaoFINAL.pdf).
- Barata, F. El relato criminal como escenario de valores y lugar de reconocimientos. In: *Medicaciones Sociales*, nº 3, II semestre 2008, pp. 19 – 40 (2008).
- \_\_\_\_\_. Los mass media y el pensamiento criminológico. In: BERGALLI, R. (coordinador). *Sistema penal y problemas sociales*, Tirant lo Blanch: Valencia (2003).
- Baratta, A. Filósofo de uma criminologia crítica. In: *Mídia e Violência Urbana*. Rio de Janeiro: Faperj (1994).
- WARREN, S; BRANDEIS, L. The Right to privacy. *Harvard Law Review*. Vol. 4. No. 5 (Dec 15, 1890), pp. 193-220. Disponível em: <https://www.cs.cornell.edu/~shmat/courses/cs5436/warren-brandeis.pdf>.
- Buolamwini, J. Como eu luto contra o preconceito em algoritmo. *TED Talk*, TEDxBeaconStreet, novembro de 2016. Acesso em 10 de janeiro de 2021. Disponível em: [https://www.ted.com/talks/joy\\_buolamwini\\_how\\_i\\_m\\_fighting\\_bias\\_in\\_algorithms?language=pt-t-206129](https://www.ted.com/talks/joy_buolamwini_how_i_m_fighting_bias_in_algorithms?language=pt-t-206129)
- Cerqueira, C. M. N. O comandante de uma polícia brasileira. In: *Mídia e Violência Urbana*. Rio de Janeiro: Faperj (1994).
- Doneda, D. *Da privacidade à proteção de dados pessoais*: elementos de formação da Lei geral de proteção de dados. 2ª ed. São Paulo: Thomson Reuters Brasil (2019).
- \_\_\_\_\_. A proteção dos dados pessoais como um direito fundamental. *Espaço Jurídico Journal of Law [EJLL]*, v. 12, n. 2, p. 91-108 (2011).
- Frazão, A. Fundamentos da proteção dos dados pessoais – Noções introdutórias para a compreensão da importância da Lei Geral de Proteção de Dados. In: *Lei geral de proteção de dados pessoais e suas repercussões no direito brasileiro*. Frazão, A.; Tepedino, G.; Oliva, M. D.. 2ª ed. São Paulo: Thomson Reuters Brasil (2020).
- Instituto Igarapé. *Reconhecimento Facial no Brasil*. Acesso em 05 de janeiro de 2021. Disponível em: <https://igarape.org.br/infografico-reconhecimento-facial-no-brasil/>.
- Kurbalija, J. *Uma introdução à governança da internet*. Disponível em: [https://cgi.br/media/docs/publicacoes/1/CadernoCGIbr\\_Uma\\_Introducao\\_a\\_Governanca\\_da\\_Internet.pdf](https://cgi.br/media/docs/publicacoes/1/CadernoCGIbr_Uma_Introducao_a_Governanca_da_Internet.pdf).
- Lei Federal nº 12965, de 23 de abril de 2014. (2014). Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil (Marco Civil da Internet). Acesso em 03 de janeiro de 2021. Disponível em: [http://www.planalto.gov.br/ccivil\\_03/\\_ato2011-2014/2014/lei/l12965.htm](http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm).
- Lei Federal nº 13709, de 14 de agosto de 2018. (2018). Lei Geral de Proteção de Dados (LGPD). Acesso em 03 de janeiro de 2021. Disponível em: [http://www.planalto.gov.br/ccivil\\_03/\\_ato2015-2018/2018/lei/L13709.htm](http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm).
- LGPD Penal: Proteção de dados pessoais, segurança pública e investigações. Palestra realizada pelo Data Privacy Brasil (2020). Acesso em 08 de janeiro de 2021. Disponível em em: <https://www.youtube.com/watch?v=ZCnvMtPtDho>

- Nunes, P. Levantamento revela que 90,5% dos presos por monitoramento facial no Brasil são negros. *Intercept Brasil* (2019). Acesso em 11 de janeiro de 2021. Disponível em: <https://theintercept.com/2019/11/21/presos-monitoramento-facial-brasil-negros/>.
- \_\_\_\_\_. O algoritmo e racismo de cada dia. *Revista Piauí* (2021). Acesso em 13 de janeiro de 2021. Disponível em: <https://piaui.folha.uol.com.br/o-algoritmo-e-racismo-nosso-de-cada-dia/>.
- Silva, P. G. F. da. Sorria você está sendo reconhecido: o reconhecimento facial como violador de direitos humanos? *ITS Rio Feed* (2020). Acesso em 05 de janeiro de 2021. Disponível em: <https://feed.itsrio.org/sorria-voc%C3%AA-est%C3%A1-sendo-reconhecido-o-reconhecimento-facial-como-violador-de-direitos-humanos-4113914441d3>.
- Silva, T. da. Visão Computacional e racismo algorítmico: branquitude e opacidade no aprendizado de máquina. *Revista da Associação Brasileira de Pesquisadores/as Negros/as (ABPN)*, s.l., v. 12, n. 31, (2020). Acesso em 11 de janeiro de 2021. Disponível em: <https://abpnrevista.org.br/index.php/site/article/view/744>.

## Notas finais

1 É claro que é um desafio legislar ou estabelecer outros mecanismos regulatórios para a internet diante de contextos inerentes ao seu próprio funcionamento, como a ausência de fronteiras físicas e a rápida propagação de informação.

2 Importante destacar que o Marco Civil da Internet foi fruto de uma ação conjunta desenvolvida pelo então Ministério da Justiça e a Fundação Getúlio Vargas do Rio de Janeiro, especificamente o Centro de Tecnologia e Sociedade da Faculdade de Direito da FGV Rio, que elaboraram a minuta da legislação e submeteram a consulta pública para estimular a participação popular antes de enviar ao Congresso Nacional.

3 Art. 3º A disciplina do uso da internet no Brasil tem os seguintes princípios: (...) II - proteção da privacidade; III - proteção dos dados pessoais, na forma da lei;

4 O art. 5º, II da LGPD aponta que “Para os fins desta Lei, considera-se: dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural.”

5 Pela LGPD, o tratamento é qualquer operação realizada com dados. O art. 5º, X da LGPD estabelece que “X - tratamento: toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento,

armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.”

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

7 Hoje, a maioria dos programadores é branca e heterossexual, o que não contribui para a diversidade nos times. Os programadores treinam a inteligência artificial conforme a sua visão de vida fornecendo os parâmetros (banco de dados) conforme o que eles conhecem. Por isso é importante estimular que pessoas de grupos minoritários também possam atuar na área de tecnologia contribuindo para a diversidade de perspectivas no desenvolvimento dos softwares e nos próprios resultados da tecnologia. A pesquisa #QuemCodaBR realizada pela PretaLab e ThoughtWorks em 2018 e 2019 apresenta alguns dados interessante sobre a questão no país: somente 36.9% das equipes é composta por uma pessoa Negra/Preta/Parda, 68% de todos os times analisados são homens; 78% dos entrevistados é heterossexual; somente 1,6% dos times são pessoas com deficiência; 62% das equipes não tem nenhum mulher mãe; em 68,5% das equipes as pessoas negras representam o máximo de 10% das pessoas nas equipes de trabalho em tecnologia. Disponível em: [https://assets-global.website-files.com/5bo5e2erbfcfaa4f92e2ac3a/5d671881e1161a6d2b8eb78b\\_Pesquisa%20QuemCodaBR.pdf](https://assets-global.website-files.com/5bo5e2erbfcfaa4f92e2ac3a/5d671881e1161a6d2b8eb78b_Pesquisa%20QuemCodaBR.pdf). Acesso em: 11.01.2021.

8 Art. 4º Esta Lei não se aplica ao tratamento de dados pessoais: (...) III - realizado para fins exclusivos de: a) segurança pública; b) defesa nacional; c)



segurança do Estado; ou d) atividades de investigação e repressão de infrações penais; (...)  
§ 1º O tratamento de dados pessoais previsto no inciso III será regido por legislação específica, que deverá prever medidas proporcionais e estritamente necessárias ao atendimento do interesse público, observados o devido processo legal, os princípios gerais de proteção e os direitos do titular previstos nesta Lei.

9 A Comissão de Juristas foi composta por Nefi Cordeiro (presidente), Antonio Saldanha Palheiro (vice-presidente), Laura Schertel Mendes (relatora), Pedro Ivo Velloso (secretário), Danilo Doneda, Davi Tangerino, Eduardo Queiroz, Heloisa Estellita, Humberto Fabretti, Ingo Sarlet, Jacqueline Abreu, Jorge Octávio Lavocat Galvão, Juliana Abrusio, Tércio Sampaio Ferraz Júnior e Vladimir Aras.

10 A função dessa legislação é primordial para alinhar proteção de dados, direitos fundamentais e segurança pública. Como citada na própria exposição de motivos do anteprojeto “trata-se, portanto, de projeto que oferece balizas e parâmetros para operações de tratamento de dados pessoais no âmbito de atividades de segurança pública e de persecução criminal, equilibrando tanto a proteção do titular contra mau uso e abusos como acesso de autoridades a todo potencial de ferramentas e plataformas modernas para segurança pública e investigações.”

11 Na palestra realizada pelo Data Privacy Brasil em 27 novembro de 2020 sob o título “LGPD Penal: Proteção de dados pessoais, segurança pública e investigações”, Jacqueline Abreu e Laura Schertel, respectivamente membro da Comissão e relatora do anteprojeto, realizaram uma série de esclarecimentos acerca da avaliação de risco da atividade e a avaliação de impacto regulatório nos minutos 23 a 30. Disponível em: <https://www.youtube.com/watch?v=ZCnvMtPtDho>. Acesso em: 08.01.2021.

12 Importante mencionar que a exposição de motivos do anteprojeto explica o motivo do papel fiscalizador atribuído ao CNJ no uso do reconhecimento facial e segurança pública nos seguintes termos: “A escolha do CNJ como a autoridade responsável deu-se em razão da sua autonomia e da pluralidade de sua composição. Sabe-se que a autonomia e imparcialidade do órgão supervisor é fundamental para que um país esteja apto a pleitear uma decisão quanto à adequação de sua legislação de proteção de dados ao nível de proteção europeu, que permitiria às autoridades de investigação no país acessar e compartilhar uma maior quantidade de dados com autoridades e instituições europeias, como Europol, Interpol e Eurojust. Dessa forma, a indicação do CNJ como órgão supervisor é importante na medida em que (i) evita o dispêndio de novos gastos com a criação de um órgão específico; (ii) aproveita a expertise dos setores, dos Conselheiros e dos servidores do CNJ que já vêm expedindo atos normativos importantes sobre a proteção de dados no âmbito brasileiro (v.g. Recomendação CNJ n. 73, de 20/8/2020 e Portaria CNJ n. 63/2019); e (iii) permite a formulação de políticas públicas uniformes para todo território nacional, a partir de uma composição plural e independente com membros de instituições diversas à luz do art. 103-B, da Constituição Federal (v.g. Poder Judiciário estadual, federal e trabalhista, Ministério Público estadual e federal, Ordem dos Advogados do Brasil, Câmara dos Deputados e Senado Federal.”

13 Na palestra realizada pelo Data Privacy Brasil em 27 novembro de 2020 sob o título “LGPD Penal: Proteção de dados pessoais, segurança pública e investigações”, Jacqueline Abreu e Laura Schertel, respectivamente membro da Comissão e relatora do anteprojeto, realizaram esclarecimentos acerca do art. 43 nos minutos 50 a 53. Disponível em: <https://www.youtube.com/watch?v=ZCnvMtPtDho>. Acesso em: 08.01.2021.

14 Disponível em: <https://acervo.folha.com.br/index.do>. Acesso em: 09.01.2021.

15 Inicialmente, o site informa 38 resultados, mas percebeu-se que três dos resultados são duplicados, em outros dois não havia menção alguma ao termo de busca e outras duas menções somente tratam de chamada para outra reportagem sobre o tema.

16 Os demais assuntos tratados foram 16 (dezesesseis) sobre aplicação no comércio (moda, alimentos, smartfones, curso, brinquedo, pagamento, doação de sêmen), 3 (três) sobre críticas ao reconhecimento facial como um todo (software que pretendia identificar rosto de pessoas homossexuais, armazenamento indevido de dados de reconhecimento facial pelo Facebook), 2 (dois) sobre aplicação no serviço público (conservação da cidade, identificação de cadáver), 2 (dois) sobre tendências anuais, 1 (um) sobre cibersegurança, 1 (um) utilização no mercado de trabalho, 4 (quatro) sobre segurança pública, 1 (um) sobre uso em aeroporto, 1 (um) sobre acessibilidade.

17 Disponível em: <https://acervo.folha.com.br/leitor.do?numero=48044&keyword=%22reconhecimento+facial%22&anchor=6069133&origem=busca&originURL=&pd=1eb395bb2efb6912f89680c93cc75c7d>. Acesso em: 09.01.2021.

18 Disponível em: <https://acervo.folha.com.br/leitor.do?numero=48244&keyword=%22reconhecimento+facial%22&anchor=6083793&origem=busca&originURL=&pd=6a573db583ca4f4799b571b53bb56fa9>. Acesso em: 09.01.2021.

19 Disponível em: <https://acervo.folha.com.br/leitor.do?numero=48274&keyword=%22reconhecimento+facial%22&anchor=6086208&origem=busca&originURL=&pd=102b5195187fc86841boarod946boobc>. Acesso em: 09.01.2021.

20 Inicialmente, o site informa 66 resultados, mas percebeu-se que treze dos resultados são duplicados, em outros oito não havia menção alguma ao termo de busca e outras três menções somente tratam de chamada para outra reportagem sobre o tema.

21 Os demais resultados foram somente 15 (quinze) sobre aplicação no comércio (carros, bancos, companhia aérea, aplicativos de transporte, startup, leitor de emoção, celular, restaurante), 5 (cinco) sobre críticas ao uso indevido da inteligência artificial, 12 (doze) sobre aplicação no serviço público (transporte, intercâmbio com os países que usam o sistema, eleição), 1 (um) utilização no mercado de trabalho, 2 (dois) experiências de outros países, 2 (dois) sobre segurança pública, 1 (um) sobre aplicação no esporte, 1 (uma) menção em entrevista, 2 (dois) aplicação na arte, 1 (um) sobre tendência.

22 Disponível em: <https://acervo.folha.com.br/leitor.do?numero=48446&keyword=%22reconhecimento+facial%22&anchor=6098957&origem=busca&originURL=&pd=7cf4f779eco829496b3bodd6603daofc>. Acesso em: 09.01.2021.

23 Disponível em: <https://acervo.folha.com.br/leitor.do?numero=48815&keyword=%22reconhecimento+facial%22&anchor=6124241&origem=busca&originURL=&pd=e8b750cad4d973eda643bc17e80a7cbb>. Acesso em: 09.01.2021.

24 Inicialmente, o site informa 104 (cento e quatro) resultados, mas percebeu-se que 18 (dezoito) dos resultados são duplicados, em outros 11 (onze) não havia menção alguma ao termo de busca e outras 6 (seis) menções somente tratam de chamada para outra reportagem/recomendação sobre o tema.

25 Os demais tratam sobre 20 sobre aplicação no comércio (celular, startup, banco, leitor de emoção), 7 crítica sobre o reconhecimento

facial, 11 sobre aplicação no serviço público (monitoramento de terreno, trânsito, eleições, atendimento, transporte público), 4 utilização no mercado de trabalho, 5 experiências de outros países, 8 sobre segurança pública, 2 viés no algoritmo de reconhecimento facial, 1 sobre cibersegurança, 1 aplicação no esporte, 2 em entrevista, 2 sobre tendências, 6 aplicação para saúde pública.

26 Disponível em: <https://acervo.folha.com.br/leitor.do?numero=48924&keyword=%22reconhecimento+facial%22&anchor=6131909&origem=busca&originURL=&pd=d587cf1008d339bde00d19a72556f68e>. Acesso em: 09.01.2021.

27 Disponível em: <https://acervo.folha.com.br/leitor.do?numero=48929&keyword=%22reconhecimento+facial%22&anchor=6132245&origem=busca&originURL=&pd=a873fab7e18804d03eacaf8013d1b5f4>. Acesso em: 09.01.2021.

28 Disponível em: <https://acervo.folha.com.br/leitor.do?numero=48964&keyword=%22reconhecimento+facial%22&anchor=6135106&origem=busca&originURL=&pd=09fec6e232c59b9305727d15d14c9c3b>. Acesso: 09.01.2021.

29 Disponível em: <https://acervo.folha.com.br/leitor.do?numero=49043&keyword=%22reconhecimento+facial%22&anchor=6405626&origem=busca&originURL=&pd=164b709a829c29077ed6e507e5ae4094>. Acesso em: 09.01.2021.

30 Disponível em: <https://acervo.folha.com.br/leitor.do?numero=49066&keyword=%22reconhecimento+facial%22&anchor=6407019&origem=busca&originURL=&pd=e4958aa0330e61322b15d5b1b2b4679a>. Acesso em: 09.01.2021.

31 Disponível em: <https://acervo.folha.com.br/leitor.do?numero=49068&keyword=%22reconhecimento+facial%22&anchor=6407153&origem=busca&originURL=&pd=a0061675a02126fe2f02b628b834ce90>. Acesso em: 09.01.2021.

32 Disponível em: <https://acervo.folha.com.br/leitor.do?numero=49072&keyword=%22reconhecimento+facial%22&anchor=6407421&origem=busca&originURL=&pd=c1a85b2d0972c2141bc1b357425ed39b>. Acesso em: 09.01.2021.

33 Disponível em: <https://acervo.folha.com.br/digital/leitor.do?numero=49282&keyword=%22reconhecimento+facial%22&anchor=6419234&origem=busca&originURL=&pd=3312abb80c6058d085185fee46479e1b>. Acesso em: 09.01.2021.

34 Disponível em: <https://acervo.folha.com.br/leitor.do?numero=48935&keyword=%22reconhecimento+facial%22&anchor=6132847&origem=busca&originURL=&pd=80bd2261669e75ca43b21019725f321c>. Acesso em: 09.01.2021.

35 É importante mencionar que existe um grande lapso temporal decorrido entre as pesquisas de Carlos Magno Nazareth Cerqueira em 1994 e o presente artigo. Por conta disso, os estudos do autor não abarcam os usos da inteligência artificial na segurança pública, mas não deixa de apresentar perspectivas necessárias, importantes e fundamentais para pensar na função dos órgãos de segurança pública no combate ao crime e no papel da opinião pública e imprensa na criminologia.