PONTIFÍCIA UNIVERSIDADE CATÓLICA DE GOIÁS

ESCOLA DE DIREITO, NEGÓCIOS E COMUNICAÇÃO

NÚCLEO DE PRÁTICA JURÍDICA

COORDENAÇÃO ADJUNTA DE TRABALHO DE CURSO

ARTIGO CIENTÍFICO

APLICABILIDADE DAS TECNOLOGIAS DISRUPTIVAS DE RECONHECIMENTO FACIAL EM SISTEMAS DE VIGILÂNCIA PÚBLICA NO BRASIL: IMPLICAÇÕES DA EFETIVIDADE DO DIREITO CONSTITUCIONAL À PRIVACIDADE

ORIENTANDO: GUILHERME BRITO ARAÚJO DA SILVA

ORIENTADORA: PROF.ª. Ms. GABRIELA PUGLIESI FURTADO CALAÇA

GOIÂNIA-GO

2022

GUILHERME BRITO ARAÚJO DA SILVA

APLICABILIDADE DAS TECNOLOGIAS DISRUPTIVAS DE RECONHECIMENTO FACIAL EM SISTEMAS DE VIGILÂNCIA PÚBLICA NO BRASIL: IMPLICAÇÕES DA EFETIVIDADE DO DIREITO CONSTITUCIONAL À PRIVACIDADE

Artigo Científico apresentado à disciplina Trabalho de Curso II, da Escola de Direito, Negócios e Comunicação, Curso de Direito, da Pontifícia Universidade Católica de Goiás (PUCGOIÁS).
Orientadora: Prof.ª Ms. Gabriela Pugliesi Furtado Calaça.

GOIÂNIA-GO

2022

GUILHERME BRITO ARAÚJO DA SILVA

APLICABILIDADE DAS TECNOLOGIAS DISRUPTIVAS DE RECONHECIMENTO FACIAL EM SISTEMAS DE VIGILÂNCIA PÚBLICA NO BRASIL: IMPLICAÇÕES DA EFETIVIDADE DO DIREITO CONSTITUCIONAL À PRIVACIDADE

Data da Defesa: 08 de junho de 2022

BANCA EXAMINADORA

Orientadora: Prof.ª Ms. Gabriela Pugliesi Furtado Calaça	Nota
Examinador Convidado: Prof. Ms. Fausto Mendanha Gonzaga	Nota

AGRADECIMENTOS

Os meus mais sinceros agradecimentos a todos que me auxiliaram direta ou indiretamente na elaboração deste trabalho. Sou muito grato aos meus pais, Heurimar Brito e Maria Aparecida, por tanta dedicação, esforço, paciência, amor e confiança despendidos a mim.

Agradeço à minha orientadora e professora Ms. Gabriela Pugliesi Furtado Calaça pela disponibilidade e auxílio ao longo da elaboração do presente trabalho.

SUMÁRIO

APLICABILIDADE DAS TECNOLOGIAS DISRUPTIVAS DE RECONHECIMENTO FACIAL EM SISTEMAS DE VIGILÂNCIA PÚBLICA NO BRASIL: IMPLICAÇÕES DA EFETIVIDADE DO DIREITO CONSTITUCIONAL À PRIVACIDADE

Guilherme Brito Araújo da Silva[1]

RESUMO

O presente artigo tem por objetivo discorrer sobre o emprego de tecnologias de reconhecimento facial automatizado em câmeras de segurança pública no Brasil, analisando se a implementação dessas tecnologias, respeitam o direito constitucional à privacidade. Para tanto, foi realizada pesquisa exploratória por meio de levantamento bibliográfico em livros, artigos e sites da internet. O avanço das técnicas de inteligência artificial e de processamento de dados, numa conjuntura de exponencial aumento da demanda mundial por segurança pública, impulsionou o uso das tecnologias de reconhecimento facial nos sistemas de vigilância pública, consistindo numa expectativa promissora de combate ao crime. Ocorre que, referidas tecnologias estão sendo implementadas no Brasil, sem contudo, possuir uma legislação que regulamente o seu uso. Em conclusão, as tecnologias de reconhecimento facial estão sendo utilizadas sem a devida transparência dos seus resultados e o seu uso pode implicar em riscos como erros de acurácia, vigilância massiva e vieses no algoritmo que podem atentar contra direitos fundamentais, como o direito à privacidade, além de ocasionar prisões indevidas. Portanto, o uso das tecnologias de reconhecimento facial, em sistemas de segurança pública no Brasil, não são compatíveis com as garantias constitucionais, por violarem direitos fundamentais dos cidadãos.

Palavras-chave: Privacidade, Segurança Pública, Reconhecimento facial.

[1] Bacharelando em Direito pela Pontifícia Universidade Católica de Goiás.

APPLICABILITY OF FACIAL RECOGNITION TECHNOLOGIES IN PUBLIC SECURITY CAMERAS: IMPLICATIONS OF EFFECTIVENESS OF THE CONSTITUCIONAL RIGTH TO PRIVACY

ABSTRACT

This article aims to discourse about the use of automated facial recognition technologies in public security cameras in Brazil, analyzing if the implementation of this technologies respect the constitucional rigth to privacy. Therefore was realized exploratory research through bibliographic survey in books, articles and websites. The advances of techniques of artificial inteligence and data processing in a conjucture of exponential increase in world demand for public security, boosted the use of facial recognition technologies in public security cameras, consisting a promising expectation of fighting crime. Otherwise this technologies are being implemented in Brazil without a legislation that regulary the use. In conclusion facial recognition Technologies are being used without the transparency of the results and the misuse can imply in risks like accuracy errors, mass surveillance and biases in the algorithm, besides attempt against fundamental rights like the right to privacy and cause undue arrests. So the use of facial recognition technologies in public security cameras in Brazil, are not compatible with the constitucional guarantees because violate fundamental rights of citizens.

Keywords: Privacy, Facial Recognition, Public Security

INTRODUÇÃO

Os estudos sobre tecnologias de reconhecimento facial datam dos anos de 1964, em uma pesquisa liderada pelo cientista Woodrow W. Bledsoe, juntamente com Helen Chan e Charles Bisson. Referida pesquisa tinha como objetivo programar computadores para reconhecer faces humanas.

O uso das tecnologias de reconhecimento facial na segurança pública de forma irrestrita em locais públicos impulsiona o surgimento de uma sociedade de vigilância digitalizada. Essa realidade assemelha-se à distopia descrita pelo ensaísta e romancista britânico George Orwell, em sua obra, intitulada “1984”. É descrita uma situação de pós-guerra, na qual imperavam três grandes estados transcontinentais num regime totalitário e de quebra da privacidade. O “Grande Irmão”, por meio das “teletelas”, uma espécie de monitor capaz de espionar a população, dispostas em locais públicos e nas casas dos cidadãos.

O termo panóptico, cunhado pelo jurista Jeremy Bentham em 1785, consiste num sistema de penitenciária ideal pelo qual o vigilante observava a todos sem ser visto. Atualmente, em razão das novas técnicas de vigilância advindas dos avanços tecnológicos, é razoável deduzir, conforme define Zygmunt Bauman que impera o pós-panóptico. Trata-se de uma vigilância líquida, imperceptível, fundada na fluidez das relações entre cidadãos e instituições, realizada especialmente por câmeras de vigilância. Nesse cenário é perceptível um gradual esvaziamento da privacidade, especialmente frente ao uso de inúmeras tecnologias que, cotidianamente, promovem intervenções na esfera privada.

O presente trabalho tem por objetivo pesquisar e refletir sobre a aplicação das tecnologias de reconhecimento facial na segurança pública, analisando sua relação com o direito à privacidade, bem como se o uso dessas tecnologias na segurança pela administração pública consiste numa atividade constitucional ou inconstitucional.

Portanto, apresenta-se o seguinte problema: há efetiva tutela do direito fundamental à privacidade frente ao uso das tecnologias de reconhecimento facial baseadas em inteligência artificial nos sistemas de vigilância pública no Brasil? A hipótese levantada é a de que tais tecnologias atentam contra o direito fundamental à privacidade previsto no artigo 5º, inciso X, da Constituição Federal de 1988.

1 DIREITO FUNDAMENTAL À PRIVACIDADE

1.1 ORIGEM E EVOLUÇÃO HISTÓRICA DA TUTELA DA PRIVACIDADE

A doutrina moderna relativa ao direito à privacidade surgiu no ano de 1890, fruto de uma publicação, na *Havard Law Review,* do ensaio denominado *"The right to privacy"*, de autoria de Samuel D. Warren e Louis Brandeis.

Entretanto, anteriormente à publicação do artigo, já era observado traços daquilo que seria definido como o direito à privacidade. Ressalta-se que o jurista Thomas McIntyre Cooley, cunhou, no ano de 1888, a expressão *"the right to be let alone*" (ZANON *apud* CANCELIER, 2017, p. 5).

O artigo de Warren e Brandeis, surgiu da divulgação exagerada de informações, nos jornais de Boston, sobre o casamento da filha de Samuel D. Warren e tinha como objetivo fundamentar o direito à privacidade, desvinculando-o do direito de propriedade.

Os autores desenvolveram o significado da expressão do direito de ser deixado só "*right to be let alone"* e reconheceram na *common law* um direito geral à privacidade, ao examinar precedentes jurisprudenciais, referentes à propriedade, direitos autorais e difamação, concluíram que o princípio a ser seguido na tutela da privacidade não perpassa pela propriedade privada, mas pela chamada *inviolate personality*[2] (DONEDA, 2020, p. 90).

Entretanto, deve-se ter cautela, ao mencionar o artigo de Warren e Brandeis, em comparação com o direito brasileiro. Isso porque referido artigo foi escrito e pensado num ambiente cultural e jurídico muito diferente do nosso, pois na jurisprudência norte-americana, fundada na *common law,* o "*right to privacy"* possui caráter geral*,* ou seja, um direito geral de personalidade (DONEDA, 2020, p. 90-91).

Em seus primórdios, a privacidade consistia num individualismo exacerbado e até egoísta. A esse período remonta a ideia da ausência de comunicação entre as pessoas (DONEDA, 2020, p. 31).

Na Idade média, com o declínio da sociedade feudal e a ascensão da classe burguesa, o burguês apropriou dos espaços, levantando barreiras, buscando a

[2] Cada indivíduo possui uma esfera pessoal inviolável, na medida em que ele tem o direito de escolher compartilhar com terceiros informações relativas a aspectos de sua personalidade e de sua vida íntima. (SAITO, 2021, P. 56).

individualidade, necessitando de intimidade (RODOTÀ, *apud* CANCELIER, 2017, p. 216). Assim, viver com privacidade tornou-se um hábito dos mais abastados (DONEDA *apud* CANCELIER, 2017, p. 215).

A preocupação com a vida privada e a intimidade fez emergir a necessidade de tutela e no século XIX surgiram os primeiros traços do direito à privacidade (CANCELIER, 2017, p. 216).

Já no Século XX, no período pós-Segunda Grande Guerra há a positivação do direito à intimidade e à privacidade. Desde então, estão sendo debatidos, em âmbito jurídico mundial, o direito fundamental da inviolabilidade à intimidade e à vida privada (SANTOS, CABRAL, 2020, p. 6).

Observa-se que, finda a Segunda Grande Guerra, a privacidade está presente em diversas declarações internacionais de direitos. Inicialmente, constata-se a primeira referência na Declaração Americana dos Direitos e Deveres do Homem em 1948, na Declaração Universal dos Direitos do Homem, aprovada pela Assembleia Geral das Nações Unidas, também em 1948; bem como na Convenção Europeia dos Direitos do Homem, de 1950, na Convenção Americana dos Direitos do Homem de 1969 e, recentemente, na Carta dos Direitos Fundamentais da União Europeia de 2000 (DONEDA, 2020, p. 97).

Durante a década de 1960 houve um exponencial desenvolvimento das tecnologia de coleta e sensoriamento de informações, fato que ocasionou um distanciamento do direito à privacidade de suas origens. (DONEDA *apud* CANCELIER, 2017, p. 219). Ademais ao longo do século XX, houve mudanças entre os espaços públicos e privados das sociedades e indivíduos, o que democratizou o interesse pela tutela da privacidade, bem como o seu exercício (CANCELIER, 2017, p. 219).

1.2 CONCEITO DE PRIVACIDADE

A privacidade, durante muito tempo, foi definida pela busca de alguma forma de isolamento, refúgio ou segredo. Entretanto, o conceito de privacidade, aponta para elementos, dentre outros, como a busca da igualdade, da liberdade de escolha, do anseio em não ser discriminado, à personalidade e ao seu desenvolvimento (DONEDA, 2020, p. 31).

Cumpre esclarecer que o direito à privacidade faz parte da disciplina Direito Internacional dos Direitos Humanos, sendo este um ramo do Direito Internacional Público, com surgimento logo após o fim da Segunda Guerra Mundial com o propósito de proteger direitos de todos os cidadãos, sem quaisquer discriminações de raça, cor, sexo, língua, religião, condição política, condição social entre outras características (MAZZUOLI *apud* DAVARIZ, OBREGON, 2019, p. 108).

Ademais, o direito à privacidade encontra-se nos direitos de primeira geração, que tem como marco as revoluções liberais do século XVIII, são os direitos de liberdade em sentido amplo, sendo os primeiros a constarem dos textos normativos constitucionais, a saber, os direitos civis e políticos. São direitos a prestações preponderantemente negativas, nas quais o Estado deve proteger a esfera de autonomia do indivíduo, também denominados de “direitos de defesa”, pois protegem o indivíduo contra intervenções indevidas do Estado, compreendendo-se como um dever de abstenção. Entre eles, estão os direitos às liberdades, à vida, à igualdade perante a lei, à propriedade, à intimidade, dentre outros (RAMOS *apud* ZOUEN, 2019).

A privacidade sofreu diversas transformações desde o conceito elaborado por Warren e Brandeis como o “direito a ser deixado só”, até a concepção atual, caracterizada pela liberdade de autodeterminação informativa, ou seja, a capacidade de controlar as informações pessoais pelo seu titular (MACHADO, 2014, p. 339).

Por essa razão, a privacidade deve ser compreendida a partir do nosso tempo, com os inúmeros fluxos de dados dos últimos anos e o processamento massivo de informações e não do que ela representou para outras sociedades (DONEDA, 2020, p. 92).

Em âmbito Internacional também não há uma definição precisa e inequívoca para a privacidade, visto que o Tribunal Europeu de Direitos Humanos não considera possível, nem necessário, procurar uma definição exaustiva para a noção de vida privada (LEONARDI *apud* SPALE, REIS, 2018, p. 23).

Ainda, o direito à privacidade não pode ser entendido como um direito subjetivo ou escolha pessoal, na qual o indivíduo poderia renunciar a esse direito. Por se tratar de um direito fundamental, possui como características a inalienabilidade, indisponibilidade e Imprescritibilidade. Assim, a tutela da privacidade pode ser melhor enquadrada como uma situação que não se expressa através do exercício arbitrário do poder do seu titular, mas num complexo de interesses, tanto do titular quanto da

coletividade, que pode originar poderes e deveres. Assim, a tutela da privacidade seria uma situação subjetiva complexa (PERLINGIERI *apud* DONEDA, 2020, p. 95).

Marcel Leonardi assevera que a privacidade pode ser bipartida em dois grupos: i) Conceitos unitários, que buscam a essência ou núcleo comum às situações fáticas; ii) Conceitos plurais, que entendem a privacidade como proteções heterogêneas contra problemas distintos parcialmente conectados. Os conceitos unitários podem ser subdivididos em quatro categorias gerais, são elas: a) O direito de ser deixado só, teorizado pelos advogados Samuel Warren e Louis Brandeis, no qual o acesso não consentido de terceiros aos fatos íntimos do indivíduo implicaria num dano psíquico e consequentemente num dano à personalidade do indivíduo; b) resguardo contra interferências alheias, ou seja, uma proteção da intimidade contra intrusões indesejadas pelo indivíduo; c) segredo ou sigilo, no qual busca a proteção absoluta de determinadas informações do indivíduo contra a exposição indesejada; d) controle sobre informações e dados pessoais, desenvolvida a partir da década de 1960, devido a globalização das tecnologias de informação, comunicação e inovações tecnológicas que possibilitaram o uso indevido, ilícito e perigoso dos dados coletados, bem como o monitoramento massivo da população (LEONARDI *apud* OLIVEIRA, RODRIGUES, 2020 p. 45-47).

Atualmente há de reconhecer um gradual esvaziamento da privacidade, entretanto, não há falar que não existam espaços de maior tutela e mecanismos de reparação para eventuais intromissões na esfera privada (SARLET; MARINONI; MITIDIERO, *apud* SANTOS, CABRAL. 2020, p. 11).

1.3 PREVISÃO DO DIREITO À PRIVACIDADE NA CONSTITUIÇÃO FEDERAL DE 1988

O direito à privacidade está no catálogo dos direitos individuais da Constituição da República Federativa do Brasil, no artigo 5º, inciso X, tutelando que “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” (MENDES, BRANCO, 2021, p. 547). Além disso no Brasil, existem tratados internacionais de direitos humanos como o Pacto Internacional de Direitos Civis e

Políticos, a Convenção Americana de Direitos Humanos, bem como a Lei do Marco Civil da Internet e a Lei Geral de Proteção de Dados Pessoais.

A Constituição Federal de 1988 adotou as expressões “intimidade” e “vida privada”, compreendendo que a proteção da pessoa humana abrange ambos os termos (MACHADO, 2014, p. 339).

A intimidade consiste na essência do indivíduo e a sua personalidade, como questões da vida amorosa, opção sexual, diário íntimo e convicções (CUNHA apud ROCHAEL, 2010, p. 98). A vida privada é tratada com devida reserva, e se relaciona com as questões familiares, com os relacionamentos no trabalho e com os amigos (ROCHAEL, 2010, p. 98).

A partir da análise das expressões “vida privada” e “intimidade”, observa-se que ambas possuem o mesmo objetivo, qual seja, proteger a pessoa humana com maior amplitude possível, observando a complexidade das situações existentes (MACHADO, 2014, p. 339-340).

2 TECNOLOGIAS DE RECONHECIMENTO FACIAL

2.1 CONCEITO E FUNCIONAMENTO DAS TECNOLOGIAS DE RECONHECIMENTO FACIAL

Reconhecimento facial consiste numa das categorias de segurança biométrica, por meio da qual identifica ou confirma a identidade de uma pessoa a partir da análise do rosto. As tecnologias de reconhecimento facial podem ser usadas para identificar pessoas em tempo real, em fotos ou vídeos (KASPERSKY).

Essas tecnologias funcionam por meio da análise de informações da face para mapear características faciais de uma pessoa, comparando as informações obtidas com um banco de dados de rostos conhecidos, objetivando encontrar uma correspondência. Em geral, o processo ocorre em quatro etapas. Na primeira etapa a câmera detecta o rosto, a partir de uma foto ou vídeo. Posteriormente, o *software* faz a leitura dos dados geométricos do rosto detectado, identificando fatores como a distância entre os olhos e a distância da testa ao queixo, com o objetivo de identificar os principais pontos de referência facial que o individualizam, e elabora um código denominado de “assinatura facial” (COSTA, OLIVEIRA. 2019, p. 87).

Na terceira etapa, haverá a comparação da face individualizada, por meio de uma fórmula matemática, com um banco de dados que contém imagens de faces armazenadas, no qual haverá um código numérico para cada pessoa analisada, chamado de impressão facial (COSTA, OLIVEIRA. 2019, p. 87).

Por último, o código numérico da impressão facial é comparado com outros códigos já armazenados em um banco de dados com o objetivo de ocorrer a localização de uma correspondência. Assim, caso a impressão facial corresponda a uma imagem armazenada no banco de dados, ocorrerá uma determinação e será possível identificar uma pessoa de forma automatizada.

2.2 HISTÓRICO DO RECONHECIMENTO FACIAL

Os primeiros resultados de pesquisas com o reconhecimento da face são do matemático Woodrow Bledsoe e datam de 1964. Foram realizadas medições da distâncias entre características faciais, como nariz, boca, olhos, dentre outros, antes do programa de computador calcular distâncias e raios para um ponto de referência comum. Esse ponto de referência era depois comparado com os dados disponíveis para identificar um suspeito constante num livro de fotos.

Em 1996, o governo norte-americano reconheceu e adotou o rosto como um atributo biométrico não invasivo. Esse posicionamento do governo permitiu a viabilidade comercial da tecnologia, ocasionando o surgimento do programa de Tecnologia de Reconhecimento Facial (FERET), o primeiro conjunto de dados faciais em grande escala disponível para pesquisa acadêmica e comercial. Já na década de 1970, Goldstein, Harmon, e Lesk utilizaram identificadores específicos para automatizarem o reconhecimento (SINFIC).

Na década de 2000, houve uma demanda por mais dados para pesquisas acadêmicas e comerciais. Nesse mesmo período foi realizado um teste experimental no *January 2001 Super Bowl*. O teste coletou imagens das câmeras de vigilâncias e realizou uma comparação com as imagens constantes na base de dados. Tal demonstração fez surgir uma análise sobre a forma de utilizar a tecnologia com o objetivo de atender determinadas necessidades nacionais e, ao mesmo tempo, as preocupações da sociedade relativas à privacidade (SINFIC).

Com o objetivo de aprimorar a tecnologia, houve um aumento na procura de novos métodos e mais dados. A última era do reconhecimento facial datada de 2014 até os dias de hoje, ocorreu em razão da popularização da inteligência artificial[3].

Assim, a implementação da inteligência artificial nas tecnologias de reconhecimento facial, foi um grande avanço, uma vez que as imagens constantes em bancos de dados digitais são processadas por meio de algoritmos, ocasionando um expressivo aumento da capacidade de processamento e de conexão dos dados existentes. (NORRIS, *apud* NEGRI, OLIVEIRA, COSTA, 2020, p. 6-7).

2.3 O PANÓPTICO NA SOCIEDADE DE VIGILÂNCIA

O termo panóptico, foi cunhado pelo jurista Jeremy Bentham em 1785 e consiste num sistema de penitenciária ideal. É formado por um edifício circular, com celas vazadas e uma torre no centro, que permite ao vigilante observar todos os prisioneiros, sem que estes saibam que estão, ou não, sendo observados, imprimindo um sentimento de vigilância permanente sobre os presos.

Para Byung-Chul Han, filósofo sul-coreano, o panóptico digital diferencia-se do “Grande Irmão” de George Orwell, pois, as pessoas não se sentem realmente vigiadas ou ameaçadas na sociedade digital, pelo contrário, possuem um sentimento de liberdade. (HAN *apud* COSTA, NEGRI, OLIVEIRA. 2020, p. 88).

O panóptico digital possibilita uma vigilância digitalizada, a partir de qualquer ângulo, sendo muito mais eficiente pois elimina pontos cegos. (HAN *apud* COSTA, NEGRI, OLIVEIRA. 2020, p. 89).

A partir do século XVIII, a vigilância consiste num dos principais dispositivos para o exercício do poder e, ao longo do tempo, vem tornando-se cada vez mais ampliada e aperfeiçoada para promover processos de coerção aos sujeitos sob vigilância. (PESSOA, 2020, p. 28).

---

[3] Por inteligência artificial, faz-se oportuna menção à definição trazida por John McCarthy, que a define como “a ciência e a engenharia de fabricar máquinas inteligentes, especialmente programas de computadores inteligentes. Está relacionada à tarefa semelhante de usar computadores para entender a Inteligência humana, mas a IA não precisa se limitar aos métodos biologicamente observáveis”. (MACCARTHY *apud* IBM, 2020).

Assim, em razão do aperfeiçoamento das tecnologias de informação e comunicação nos dias atuais, é razoável deduzir que vivenciamos um pós-pan-óptico, conforme definição de Zygmunt Bauman, no qual as novas formas de vigilância, advindas com avanços tecnológicos imprime uma vigilância líquida, fundada na fluidez das relações entre sujeitos e instituições, possibilitando a volatilidade do olhar vigilante (BAUMAN *apud* PESSOA, 2020, p. 46).

Ainda, conforme assevera Didier Bigo, no que tange à segurança nacional, há a existência de um banóptico, definindo quem será colocado sob vigilância pelos agentes de segurança pública (BIGO *apud* PESSOA, 2020, p. 46).

3 O USO DAS TECNOLOGIAS DE RECONHECIMENTO FACIAL NO BRASIL

3.1 SEGURANÇA PÚBLICA NO BRASIL

O uso das tecnologias de reconhecimento facial nos sistemas de vigilância pública, consiste numa tendência mundial, consequência dos avanços das técnicas de inteligência artificial e de processamento de dados, juntamente com uma elevada demanda mundial por segurança.

Na América Latina, a expansão do uso de videomonitoramento urbano advém como uma resposta ao problema da violência. Referidas tecnologias comumente são aliadas ao setor público para serem aplicadas na segurança pública. Argumenta-se que quando empregadas em conjunto com eficientes processos e práticas de policiamento podem atuar como meios de prevenção ao crime (FRANCISCO, HUREL, RIELL, 2020 p. 2).

O tema da segurança pública é considerado altamente relevante no Brasil, visto que desde a primeira Constituição Política do Império de 1824, no artigo 102, inciso XV, atribuía ao imperador a função de promover a segurança interna e externa do país (BRASIL, 1824. Art. 102, inciso XV).

A Constituição Federal de 1988, assegura no artigo 6º o direito social à segurança, de modo a demandar do Poder Público a prestação de condições que possibilitam a percepção de ordem social e preservação do indivíduo e seus bens (BRASIL, 1988, Art. 6º). Ainda, o texto constitucional é explícito ao dispor no artigo 144 a segurança pública como um dever do Estado, direito e responsabilidade de

todos, sendo exercida com o objetivo de preservar a ordem pública, a segurança das pessoas e do patrimônio (BRASIL, 1.988, Art. 144).

Nos últimos anos, o uso de sistemas de reconhecimento facial em câmeras de vigilância pública elevou os níveis da política de monitoramento. Alguns entes estatais consideram referida tecnologia como o método mais eficiente de “gestão de risco” e o seu uso é justificado a partir dos números relativos à criminalidade e violência no país (PISANU, Gaspar *et al*., 2021, p. 43), mesmo com poucos esclarecimentos a respeito das precauções para reduzir a restrição a direitos fundamentais como a liberdade de expressão, a privacidade e a proteção de dados pessoais (BOTELLO *apud* FRANQUEIRA, HARTMANN, SILVA, 2021, p. 174).

3.2 CASOS DE IMPLEMENTAÇÃO DAS TECNOLOGIAS DE RECONHECIMENTO FACIAL NO BRASIL

Segundo o Instituto Igarapé os casos reportados de uso das tecnologias de Reconhecimento Facial no Brasil somam 48 e datam desde 2011 (FRANCISCO, HUREL, RIELLI, 2020, p. 13). Entretanto, apesar do aumento no uso dessas tecnologias pela Administração Pública no Brasil, não há uma legislação de âmbito nacional sobre o tema e raros sãos os entes da federação que possuem uma legislação que estabeleça parâmetros para o uso dessas tecnologias na segurança pública. Ocorre que no contexto da Administração Pública, a lei é o limite do que é permitido, ou não, fazer, devendo sempre observar o ordenamento jurídico. (REIS, ALMEIDA, SILVA, DOURADO, 2021 p. 18).

No Brasil, destaca-se as regiões Nordeste (NE) e Sudeste (SE), como os locais onde as tecnologias de reconhecimento facial são constantemente utilizadas na segurança pública, em aeroportos, ruas, praças e estádios, bem como em eventos públicos.

Dentre os casos da região Nordeste, em Salvador, durante as festividades de carnaval no ano de 2020, foram utilizadas mais de 80 câmeras que capturaram 4,3 milhões de dados faciais e o aparato policial deteve 42 pessoas foragidas, sendo que 13 estavam relacionados ao tráfico de drogas, 14 procurados por roubo, 3 por furto, 2 envolvidos em homicídio e outros. Ocorre que, esse resultado foi obtido a partir da violação da “esfera informativa” de 11,7 milhões de pessoas, ou seja, mais de 278.000

vezes a quantidade de indivíduos detidos, devendo-se questionar se o custo-benefício obtido com a tecnologia vale o risco que ela impõe à privacidade, sob a adoção da vigilância massiva pelo Estado (REIS, ALMEIDA, SILVA, DOURADO, 2021 p. 38).

Em Feira de Santana, foram obtidos 1,3 milhões de registros faciais e 33 pessoas foram detidas (PISANU, Gaspar *et al*., 2021, p. 48). No estado do Ceará, a força policial, utiliza smartphones que capturam o rosto dos suspeitos e a foto obtida é comparada com um banco de dados da Secretaria de Segurança Pública.

Já na região Sudeste, destacam-se o Rio de Janeiro e São Paulo. No Rio de Janeiro, a tecnologia de reconhecimento facial foi testada em dois eventos públicos, durante as festividades do carnaval de 2019 e na Copa América de 2019.

Em São Paulo, foram utilizadas no carnaval de 2020, assim como em investigações criminais (PISANU, Gaspar *et al*., 2021, p. 48-49).

Portanto, apesar da expansão do uso de tecnologias de reconhecimento facial nos sistema de vigilância empregados pelo setor público brasileiro, este não possui as respectivas ferramentas que possibilitem a análise objetiva dos riscos relativos à sua implementação (REIS, ALMEIDA, SILVA, DOURADO, 2021 p. 30).

3.2.1 Modalidade de Aquisição das Tecnologias de Reconhecimento Facial

Não há dúvida de que o Brasil consiste num mercado com grande potencial de expansão para a implementação das tecnologias de reconhecimento facial. Os fornecedores das tecnologias, na maioria das vezes, utilizam estratégias de vendas agressivas, como a procura pelas empresas aos órgãos públicos, por exemplo. Para além dessa estratégias, foram utilizadas outras modalidades como o pregão presencial ou eletrônico (PISANU, Gaspar *et al*., 2021, p. 44).

A escolha da estratégia mais agressiva foi utilizada na negociação da Huawei em Campinas; da Oi no Rio de Janeiro; da Hikvision em Salvador e em São Paulo; da STAFF em Campina Grande; e da Dahua com a Secretaria de Segurança Pública do Município de Mogi das Cruzes (REIS, ALMEIDA, SILVA, DOURADO, 2021 p. 23-24). Entretanto, não há relatos de que as autoridades utilizaram o sistema de compras tradicional, de concorrência aberta. Em alguns casos, as autoridades governamentais implantaram tecnologias "doadas" para testarem na população (PISANU, Gaspar *et al*., 2021, p. 45).

3.4 RISCOS AO USO DO RECONHECIMENTO FACIAL NOS SISTEMAS DE VIGILÂNCIA PÚBLICA NO BRASIL

No Brasil, o implemento das tecnologias de Reconhecimento Facial na segurança pública ocasiona uma constante vigilância em massa das pessoas e riscos pertinentes ao tratamento de dados, pois as informações coletadas são armazenados sem fim específico e sem a devida transparência. Além disso, tais tecnologias atentam contra direitos fundamentais, isso porque essas tecnologias afrontam o direito à privacidade, os direitos de crianças e adolescentes, a inviolabilidade da imagem e da honra, viola o princípio da presunção de inocência, bem como a liberdade de ir e vir (REIS, ALMEIDA, SILVA, DOURADO, 2021, p. 8).

Ainda, ao se falar sobre vigilância e direito penal no Brasil, faz-se mister considerar que a lente pela qual o Estado utiliza para punir os seus sujeitos “delinquentes” perpassa pelo escopo do critério racial. Assim, qualquer tecnologia com fulcro de melhorar a segurança pública, além de considerar aspectos técnicos de funcionalidade, necessita observar as variáveis de raça no transcorrer do seu uso (SILVA, SILVA, 2019, p. 7).

Dentre vários riscos analisados decorrentes do uso das tecnologias de reconhecimento facial, destacam-se: (I) vigilância massiva; (II) erros de acurácia; e (III) existência de viés no algoritmo.

3.4.1 Vigilância Massiva

A utilização das tecnologias de reconhecimento facial nas câmeras em espaços públicos, potencializa uma vigilância massiva por parte do Estado que observará os locais onde o cidadão frequentou, ferindo liberdades individuais e comprometendo o desenvolvimento da personalidade e autodeterminação, além de violar direitos da personalidade e intimidade (ALMEIDA, 2020, p. 284-285).

3.4.2 Erros de Acurácia

O baixo nível de acurácia do sistema de reconhecimento facial, tanto por um equívoco na identificação de uma pessoa, quanto por não compatibilizar o sujeito

procurado com o banco de dados é extremamente prejudicial aos cidadãos, haja vista se tratar de questão relativa à segurança pública (ALMEIDA, 2020, p. 287).

Quanto aos aspectos técnicos, a iluminação, o enquadramento do rosto, a expressão facial, além da qualidade de imagem e o envelhecimento do rosto, são fatores que podem obstaculizar o regular funcionamento das tecnologias de reconhecimento facial. Ainda, alguns estudos apontam que grupos demográficos específicos de etnia, gênero e idade são comumente propícios a erros das tecnologias de reconhecimento facial (BUOLAMWINI, GEBRU *apud* ALMEIDA, 2020, p. 287).

3.4.3 Vieses no Algoritmo

Por fim, os sistemas de reconhecimento facial ainda podem apresentar um determinado viés se as faces utilizadas no treinamento do algoritmo não observarem as variações de cor e etnia da população. Assim, a taxa de precisão e acurácia será diferente quando o sistema não for treinado para a detecção daquele rosto (ICO *apud* ALMEIDA, 2020, p. 287).

Estudos realizados constatam a ocorrência de uma menor precisão quando as tecnologias de reconhecimento facial são utilizadas com o fulcro de identificar uma vasta diversidade de pessoas, em especial mulheres negras. A partir dessa constatação é necessária a produção de rigorosos métodos de auditoria sobre os padrões e métricas constantes no desempenho dessas tecnologias, com o objetivo de aumentar a transparência na utilização e desempenho do algoritmo, bem como debates sobre o uso ético dessas tecnologias (ALMEIDA, 2020, p. 290).

Referida discriminação, em decorrência da presença de viés no uso do algoritmo, torna-se ainda mais preocupante quando a finalidade da tecnologia é na seara da segurança pública. Isso porque o Brasil é um país historicamente miscigenado, com inúmeras etnias, além de possuir um sistema penal tendenciosamente racista (ALMEIDA, 2020, p. 290).

CONCLUSÃO

Do exposto, o crescente interesse em segurança pelos Estados, aliado ao desenvolvimento das tecnologias, em especial o reconhecimento facial, juntamente com avanços das técnicas de inteligência artificial e processamento de dados, consiste numa ferramenta promissora para a segurança pública.

O presente trabalho analisou se, o crescente uso pelo Estado de tecnologias de reconhecimento facial aplicadas na segurança pública, pode gerar, ou não, ofensa ao direito à privacidade, previsto como direito fundamental no inciso X do artigo 5º da Constituição Federal de 1988.

Após estudos sobre a temática, foi constatado que o uso de tecnologias de reconhecimento facial sem a promulgação de uma regulamentação à respeito sobre o tema e sem a devida transparência, ofende os princípios fundamentais constantes no direito brasileiro, como o princípio da proteção de dados do titular, do livre desenvolvimento e o direito à privacidade.

No que tange à privacidade, as técnicas de reconhecimento facial aplicadas em sistemas de vigilância em locais públicos, ocasiona uma vigilância massiva pelo Estado, comprometendo o direito à privacidade das pessoas, pois interfere na vida privada, coletando dados e monitorando os cidadãos sem o consentimento destes, de forma a atentar frontalmente contra o direito fundamental à privacidade, previsto no inciso X do artigo 5º da Constituição Federal de 1988. Portanto, apesar dessas tecnologias estarem em uso no Brasil desde 2011, não são compatíveis com as garantias constitucionais, pois, violam direitos fundamentais dos cidadãos.

Ademais, as tecnologias de reconhecimento facial aplicada na segurança pública no Brasil, possuem riscos concretos quanto ao seu uso. No presente artigo, os riscos relatados foram a vigilância massiva, os erros de acurácia e o viés do algoritmo, os quais perpetuam a discriminação de grupos socialmente marginalizados e que estão mais propícios de serem erroneamente identificados pela tecnologia.

Do exposto, o uso das tecnologias de reconhecimento facial nos sistema de vigilância pública no Brasil, trata-se de atividade inconstitucional, necessitando, portanto, de uma legislação adequada e direcionada à proteção de dados e de meios assecuratórios dos direitos fundamentais dos cidadãos, especialmente o direito constitucional à privacidade.

REFERÊNCIAS

ALMEIDA, Eduarda Costa. Reconhecimento facial e segurança pública: como garantir a proteção de dados pessoais e evitar os riscos da tecnologia. ANPR. Brasília, p. 265-289, 2020. Disponível em: http://www.anpr.org.br/images/2020/Livros/protecao_dados_pessoais_versao_eletronica.pdf. Acesso em: 27 set. 2021.

BRASIL, [Constituição (1824)]. Constituição Política do Império do Brasil, de 25 de março de 1824. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao24.htm. Acesso em: 25 ago. 2021.

BRASIL, [Constituição (1988)]. Constituição da República Federativa do Brasil de 1988. Brasília, DF: Presidência da República. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicaocompilado.htm. Acesso em 15 mar. 2022.

CANCELIER, Mikhail Vieira de Lorenzi. O direito à privacidade hoje: perspectiva histórica e o cenário brasileiro. Revista Sequencia. UFISC, Florianópolis, Santa Catarina, v. 38, n. 76, p. 213-240, set. 2017. Acesso em 07 nov. 2021.

COSTA, Ramon Silva; OLIVEIRA, Samuel Rodrigues de. Uso do Reconhecimento Facial em Sistemas de Vigilância e suas Implicações no Direito à Privacidade. Revista de Direito, Governança e Novas Tecnologias, Belém, v.5, p.1-21. 2019. Disponível em: https://indexlaw.org/index.php/revistadgnt/article/view/5777/pdf. Acesso em: 18 ago. 2022.

COSTA, Ramon Silva, NEGRI, Sergio Marcos Carvalho de Ávila, OLIVEIRA, Samuel Rodrigues de. O uso de tecnologias de Reconhecimento Facial Baseadas em Inteligência Artificial e o Direito à Proteção de Dados. RDP, Brasília, Volume 17, nº 93, p. 82-103, 2020 Disponível em: https://www.portaldeperiodicos.idp.edu.br/direitopublico/article/view/3740/Negri%3B%20Oliveira%3B%20Costa%2C%202020. Acesso em: 25 ago. 2022

DAVARIZ, Caroline Aparecida Vianna, OBREGON, Marcelo Fernando Quiroga. A proteção dos dados pessoais na internet enquanto direito humano à privacidade de tutela internacional. Revista Jurídica Derecho y Cambio Social, n. 58, p. 104-133, 2019. Disponpível em: https://dialnet.unirioja.es/descarga/articulo/7075596.pdf. Acesso em: 19 mar. 2022.

DONEDA, Danilo. Da privacidade à proteção de dados pessoais: Fundamentos da Lei Geral de Proteção de Dados. 2.ed. São Paulo: Thomson Reuters Brasil, 2020.

FRANCISCO, Pedro Augusto P., HUREL, Louise Marie, RIELLI, Mariana Marques. Regulação do reconhecimento facial no setor público. Data Privacy Brasil, 2020. Disponível em: https://igarape.org.br/wp-content/uploads/2020/06/2020-06-09-Regulao-do-reconhecimento-facial-no-setor-pblico.pdf. Acesso em: 18 ago. 2021.

FRANQUEIRA, Bruna D.; HARTMANN, Ivar A.; SILVA, Lorena A. O que os Olhos não Veem, as Câmeras Monitoram: Reconhecimento Facial para Segurança Pública e

Regulação na América Latina. Revista Digital de Direito Administrativo. vol. 8, n. 1, p. 171-204, 2021. Disponível em: https://www.revistas.usp.br/rdda/article/view/173903/168395. Acesso em: 12 set. 2021.

IBM Cloud Education. O que é inteligência artificial? Disponível em: https://www.ibm.com/br-pt/cloud/learn/what-is-artificial-intelligence. Acesso em: 13 mar. 2022.

MACHADO, Joana de Moraes Souza. A expansão do conceito de privacidade e a evolução na tecnologia de informação com o surgimento dos bancos de dados. Revista da Ajuris. Rio Grande do Sul. v. 41, n. 134, 2014. Disponível em: http://ajuris.kinghost.net/OJS2/index.php/REVAJURIS/article/viewFile/206/142. Acesso em 07 nov. 2021.

MENDES, Gilmar Ferreira, BRANCO, Paulo Gustavo Gonet. Curso de Direito Constitucional. 16.ed. São Paulo: Saraiva Educação, 2021.

OLIVEIRA, Davi Teófilo Nunes, RODRIGUES, Gustavo Ramos. Privacidade e Proteção de Dados. Apostila**.** Minicurso**.** Fundamentos do Direito e Novas Tecnologias**.** IRIS. 5ª ed. p. 45-55, 2019. Disponível em: https://irisbh.com.br/wp-content/uploads/2019/05/Apostila_minicurso_5edicao.pdf. Acesso em: 02 nov. 2021.

O que é reconhecimento facial: definição e explicação. Disponível em: https://www.kaspersky.com.br/resource-center/definitions/what-is-facial-recognition. Acesso em: 14 mar. 2022.

PESSOA, João Pedro Seefeldt. O efeito Orwell na sociedade em rede: cibersegurança, regime global de vigilância social e direito à privacidade no século XXI [recurso eletrônico]. Porto Alegre, RS: Editora Fi, 2020. Disponível em: https://www.editorafi.org/073orwell. Acesso em: 12 set. 2021.

PISANU, Gaspar *et al*. Tecnologia de Vigilância na América Latina: Feita no exterior, implantada em casa. Acessnow, 2021. Disponível em: https://www.accessnow.org/tecnologia-de-vigilancia-na-america-latina/. Acesso em: 07 nov. 2021

Reconhecimento Facial: um Pouco de História e Principais Abordagens. Disponível em: http://www.sinfic.pt/SinficWeb/displayconteudo.do2?numero=24923. 2008. Acesso em: 15 mar. 2022.

REIS, Carolina; ALMEIDA, Eduarda; DA SILVA; Felipe; DOURADO, Fernando. Relatório sobre o uso de tecnologias de reconhecimento facial e câmeras de vigilância pela administração pública no Brasil. Brasília: Laboratório de Políticas Públicas e Internet, 2021. Disponível em: https://lapin.org.br/2021/07/07/vigilancia-automatizada-uso-de-reconhecimento-facial-pela-administracao-publica-no-brasil/. Acesso em: 11 jul. 2021.

ROCHAEL, Carlos Henrique Reis. O Direito Fundamental à Privacidade Garantia Constitucional Face o Avanço das Tecnologias de Vigilância e Controle Social, 2010.

Disponível em: http://tede2.pucgoias.edu.br:8080/bitstream/tede/2773/1/CARLOS%20HENRIQUE%20REIS%20ROCHAEL.pdf. Acesso em: 25 mar. 2022.

SANTOS, Rodrigo Natálicio dos, CABRAL, Cristiane Helena de Paula Lima. Reconhecimento facial: análise a partir da Constituição brasileira e da Lei Geral de Proteção de Dados. Rev.Bras.de Direito e Gestão**,** 2020. Disponível em: https://www.gvaa.com.br/revista/index.php/RDGP/article/download/8599/8072. Acesso em: 25 out. 2021.

SAITO, Vitória Hiromi. Desafios Contemporâneos para a Tutela dos Direitos à Privacidade e aos Dados Pessoais. *Res Severa Verum Gaudium*. Ufrgs, v.5, n.2. 2021. Disponível em: https://www.seer.ufrgs.br/resseveraverumgaudium/article/viewFile/110379/61654. Acesso em: 25 mar. 2022.

SILVA, Rosane Leal da, SILVA, Fernanda dos Santos Rodrigues da. Reconhecimento Facial e Segurança Pública: Os Perigos do Uso da Tecnologia no Sistema Penal Seletivo Brasileiro. Anais do 5º Congresso Internacional de Direito e Contemporaneidade: mídias e direitos da sociedade em rede, 2019. Disponível em: https://www.ufsm.br/cursos/pos-graduacao/santa-maria/ppgd/congresso-direito-anais. Acesso em: 16 mar. 2022.

SPALE, Mayara Guibor, REIS. Rafael Almeida Oliveira. Limites do Direito Fundamental à Privacidade Frente a uma Sociedade Conectada. Revista Jurídica da Escola Superior de Advocacia da OAB-PR Ano 3 - Número 3, 2018. Disponível em: http://revistajuridica.esa.oabpr.org.br/wp-content/uploads/2018/12/revista_esa_8_11.pdf. Acesso em: 05 jan. 2022.

ZOUEN, Luís Henrique Linhares. Em que consistem e quais são as “gerações” de direitos fundamentais? Meu Jurídico.com, 2019. Disponível em: https://meusitejuridico.editorajuspodivm.com.br/2019/08/09/em-que-consistem-e-quais-sao-geracoes-de-direitos-fundamentais/. Acesso em: 08 nov. 2021.

ANEXO

Entrevista realizada com a pesquisadora Eduarda Costa Almeida[4], a respeito do uso das tecnologias de Reconhecimento Facial em sistemas de vigilância pelo pública no Brasil.

1. O que são Tecnologias de Reconhecimento Facial/ vigilância biometria?

R = São tecnologias utilizadas para identificação de pessoas a partir dos dados extraídos do rosto da pessoa. A identificação é possível a partir da comparação de dados de uma base de dados e os dados das pessoas que transitam em espaços com câmeras com essa tecnologia.

2.Como essas tecnologias funcionam?

R = A partir do tratamento de dados pessoais sensíveis, descritos no art. 11, da LGPD, como a íris, a digital, a assinatura facial, DNA e outros. Com esses dados, é possível identificar a pessoa de forma inequívoca, quando a tecnologia funciona bem.

3. As tecnologias de biometria facial impactam em quais direitos fundamentais do cidadão?

R = a depender de como for aplicada, os direitos de: liberdade de ir e vir, presunção da inocência, não discriminação, igualdade, proteção de dados, privacidade.

4. Por que devemos nos preocupar com o uso das Tecnologias de Reconhecimento Facial em sistemas de vigilância pública?

R = Por violações de direitos dos cidadãos, tratamento indevido de dados pessoais e instauração de sistema de vigilância constante que não permite o desenvolvimento da personalidade.

---

[4] Pesquisadora do Laboratório de Políticas Públicas e Internet (LAPIN). Graduanda em Direito pela Universidade de Brasília (UnB).

5. Quais são os riscos envolvidos no uso de tecnologia de vigilância biométrica pela segurança pública?

R = Violação de direitos, principalmente de grupos específicos (negros, mulheres e trans), discriminação, aprofundamento de um sistema de persecução penal e segurança pública racista.

6. Atualmente, quais regiões do Brasil implantaram essas tecnologias na segurança pública? E Como são feitas as aquisições dessas tecnologias?

R = Que eu tenho notícia, Centro-Oeste, Sul, Sudeste e Nordeste. Em regra, as tecnologias são doadas, compradas em licitação ou usadas para teste, firmados em acordos técnicos temporários.

7. O princípio da supremacia do interesse público legitima o uso dessas tecnologias, possibilitando mitigar direitos e garantias individuais, em prol da segurança pública?

R = Não, nenhum princípio é absoluto e existem limites justamente na intrusão da liberdade dos cidadãos. Ainda, não está comprovado que o interesse público está sendo atendido com o uso dessa tecnologia.

8. As Tecnologias de Reconhecimento Facial, em geral, são confiáveis e precisas?

R = Não. Existem erros que podem ter efeitos ainda mais severos quando se usa a tecnologia sem salvaguardas de segurança da informação, devida abordagem, cenário adequado e outras medidas.

9. Como acontece o controle/tratamento dos dados biométricos captados pelas tecnologia de vigilância biométrica por parte da administração pública? Esses dados são compartilhados com as empresas que desenvolveram o *software* dos sistemas de vigilância biometria?

R = A administração pública usa das bases de dados que possui, além do acesso a fotos em redes sociais e outras ferramentas. Existe um compartilhamento de dados entre as autoridades. Em regra, não há cláusulas que limite o compartilhamento de dados pessoais dos cidadãos com as empresas que

desenvolvem ferramentas, não é possível afirmar que a regra é esse compartilhamento, mas não existe restrição dessa prática.

10. O Brasil está preparado para implementar as tecnologias de reconhecimento facial na segurança pública?

R = Não, por questões que vão além das falhas da tecnologia e estão relacionados com o processo penal e segurança pública no Brasil. Além do despreparo técnico dos agentes que utilizam a tecnologia.

11. Quais legislações possuímos atualmente sobre a regulamentação do uso das tecnologias de reconhecimento facial?

R = A nível nacional, nenhuma. Existe projeto de lei nº 672/2021, que está na Câmara dos Deputados. Existe a Lei Distrital nº 6.712/2020 que regula a tecnologia de reconhecimento facial na segurança pública no Distrito Federal.

12. A Lei Geral de Proteção de Dados (Lei n.º 13.709, de 14 de agosto de 2018), aborda o tema do uso das Tecnologias de Reconhecimento Facial em sistemas de vigilância pública?

R = Sim, ela afirma que uma lei deve ser editada sobre o uso de dados pessoais na segurança pública e deve ser respeitado o direito à proteção de dados, os princípios da LGPD e o devido processo legal (art. 4º, § 1º, da LGPD).