REVISTA BRASILEIRA DE SEGURANÇA PÚBLICA

ARTIGO

OS GRANDES IRMÃOS: O USO DE TECNOLOGIAS DE RECONHECIMENTO FACIAL PARA PERSECUÇÃO PENAL

EDUARDA COSTA ALMEIDA
Estudante de direito da UnB, pesquisadora do LAPIN, pesquisadora do Observatório da LGPD/UnB e CEDIS/IDP.
País: Brasil **Estado:** Distrito Federal **Cidade:** Brasília
Email: itseduardacosta@gmail.com **ORCID:** https://orcid.org/0000-0002-0575-611X

RESUMO

Este artigo analisa o uso de câmeras de vigilância com a tecnologia de reconhecimento facial (RF) automatizado e em tempo real para tratamento de dados na segurança pública e na persecução penal. As ferramentas de RF estão cada vez mais sendo usadas para auxiliar as atividades policiais, por isso é fundamental analisar os parâmetros mínimos para um uso legítimo da tecnologia. Por meio da análise de doutrinas, legislações, relatórios de casos concretos e recomendações de autoridades de proteção de dados, este estudo busca compreender o funcionamento do RF no âmbito da segurança pública, em sentido amplo, e mapear os princípios a serem observados para mitigar danos no uso do RF nessa área específica. A Diretiva 2016/680 da União Europeia e os princípios nela elencados são direcionamentos relevantes para uma possível regulamentação brasileira do uso de dados no âmbito da segurança pública. Por fim, frisa-se os principais riscos do uso indevido do RF e os danos já causados para que a legislação brasileira se atente a esses erros.
Palavras-chave: Segurança pública. Reconhecimento facial em tempo real. Proteção de dados. Riscos. Viés algorítmico.

ABSTRACT

FACIAL RECOGNITION AND PUBLIC SAFETY: HOW TO ENSURE THE PROTECTION OF PERSONAL DATA AND AVOID THE RISKS OF TECHNOLOGY

This article analyzed the use of surveillance cameras with automated and live facial recognition (FR) technology for data processing within the scope of public security. RF tools are increasingly being used to assist police activities, so it is essential to analyze the minimum parameters for legitimate use of the technology. Through reading doctrines, legislation, case reports and recommendations from personal data protection authorities, this study sought to understand the functioning of the FR and map the principles to be observed to mitigate damage in the use of FR in public security. The Directive 2016/680 of the European Union and the principles listed therein are relevant directions for a possible Brazilian regulation of the use of data in the scope of public security. Finally, the main risks of the misuse of the FR and the damage already caused were stressed so that Brazilian legislation can pay attention to these errors.
Key-words: *Public Security. Real-Time Facial Recognition. Data Protection. Risks. Bias in the algorithm.*

Data de recebimento: 07/10/2020 – **Data de aprovação:** 07/04/2021
DOI: 10.31060/rbsp.2022.v16.n2.1377

INTRODUÇÃO

Atualmente, estamos vivendo em uma sociedade da informação, onde as pessoas estão imersas em um ambiente de uso contínuo de diferentes tecnologias que estão em constante desenvolvimento. Nesse sentido, para que as pessoas possuam acesso a espaços e serviços digitais, elas, continuamente, disponibilizam seus dados pessoais e "deixam rastros" no mundo *online*. Nessa perspectiva, nota-se que esses dados pessoais têm sido utilizados por empresas e governos para diversas finalidades, a exemplo do marketing direcionado, das identidades digitais[1] e da segurança pública, em sentido amplo, que abarca tanto a persecução penal, atividade de investigação, quanto a segurança pública em sentido estrito, atividade de prevenção de crime.

Como consequência dessa realidade, percebeu-se a relevância de uma lei que tutelasse o direito de privacidade e de proteção de dados dos cidadãos. Por isso, em 2018, o Congresso Nacional brasileiro sancionou a Lei Geral de Proteção de Dados (LGPD), que garante o tratamento de informações de forma responsável e em observância aos princípios da proteção de dados em diversos contextos.

No entanto, a LGPD não se aplica inteiramente aos casos de tratamento de dados pessoais para fins exclusivamente de segurança pública (art. 4º, III, "a"). Ela prevê que a legislação específica a ser criada deverá observar os princípios gerais de proteção de dados, os direitos do titular e o devido processo legal. Ainda, essa futura lei deverá prever medidas proporcionais e estritamente necessárias ao atendimento do interesse público (art. 4º, § 1º). Dessa forma, por mais que a tecnologia avance, é necessária regulação específica sobre o uso de inovações aplicadas ao contexto de segurança pública a fim de evitar o grande potencial de uso abusivo.

Assim, o governo brasileiro tem se movimentado para pensar em estratégias de regulamentação do uso da tecnologia de Reconhecimento Facial. A Câmara dos Deputados, em abril de 2019, realizou audiência pública na Comissão de Ciência e Tecnologia, Comunicação e Informática com participação de diversos setores da sociedade para discutir a aplicação de reconhecimento facial para manutenção da segurança pública (CÂMARA DOS DEPUTADOS, 2019). As posições defendidas foram controversas; destaca-se a preocupação de organizações da sociedade civil com a privacidade e a acurácia do sistema. Além disso, em novembro de 2019, a Câmara dos Deputados instituiu uma comissão de juristas para elaborar anteprojeto de legislação específica para o tratamento de dados pessoais no âmbito da segurança pública (JÚNIOR, 2019).

Diante do exposto, nota-se que o Estado também é entidade que utiliza e decide como utilizar as informações pessoais dos cidadãos, isto é, exerce função de controlador de dados. Ainda, busca utilizar informações dos cidadãos para promoção da segurança pública em vista do cenário de elevada violência no Brasil[2] e da relevância do tema para sociedade. Porém, esbarra-se na peculiaridade de ser um tratamento

1 *No Brasil, a Lei Nº 13.444/2017 criou o programa Identificação Civil Nacional que visa criar meios para a emissão do Documento Nacional de Identidade (DNI) digital para todos os brasileiros; essa identidade substitui outras formas de identificação que deram origem ao DNI ou nele foram mencionados.*

2 *O IPEA, órgão que registra dados sobre a violência no Brasil, aponta que, em 2017, houve 65.602 homicídios. Ainda , em 2017, 75,5% das vítimas de homicídios foram indivíduos negros, sendo que a taxa de homicídios por 100 mil negros foi de 43,1. Para mais informações, acesse: https://www.ipea.gov.br/atlasviolencia/download/19/atlas-da-violencia-2019.*

de dados pessoais para prevenção, investigação, deteção ou repressão de infrações penais ou execução de sanções penais.

O uso de instrumentos tecnológicos para auxiliar a segurança pública tem aplicações concretas já praticadas pelas autoridades estatais, como as escutas telefônicas, o uso de câmeras de vigilância CCTV[3] e o estudo estatístico para atuação policial mais eficiente em áreas e horários específicos. Além dessas ferramentas, também está em debate o uso da tecnologia de RF e se ela é um instrumento válido para complementação da atividade policial.

O uso de câmeras no carnaval do Rio de Janeiro, em 2019, com a tecnologia de reconhecimento de objetos possibilitou a recuperação de um veículo roubado. Ainda, no mesmo evento, o uso de câmeras com a tecnologia de RF deu causa à prisão de quatro pessoas que possuíam mandado de prisão em aberto (LISBOA, 2019). Em Salvador, no carnaval de 2019, um homem procurado pela polícia foi preso depois de ser identificado pelo sistema de reconhecimento facial utilizado pela polícia local (LAVADO, 2020). Outro exemplo é o da Companhia do Metropolitano de São Paulo, que publicou, em 2019, edital de licitação para implementação de um sistema de câmeras com RF para algumas linhas de metrô da cidade (METRÔ, 2019). No entanto, existem diversas controvérsias sobre a aplicação do RF que serão evidenciadas neste artigo.

No exterior, a polícia metropolitana de Londres (MET) utilizou por meses duas câmeras com RF no *King's Cross Central*, um dos locais mais visitados em Londres, sem informar às pessoas que passavam pelo local e que tiveram seus dados coletados (SABBAGH, 2019). Essa atuação levantou questionamentos que serão melhor explorados a seguir. Em São Francisco, nos Estados Unidos, o órgão governamental competente, *The Board of Supervisors*, baniu a tecnologia de RF por oito votos contra um, visto o seu alto potencial de uso abusivo e a consequência de uma vigilância opressiva e massiva (CONGER; FAUSSET; KOVALESKI, 2019). Ainda, a IBM, uma das maiores empresas de tecnologia do mundo, anunciou que deixará de investir em tecnologias de RF, já que, segundo a empresa, esse instrumento está sendo usado, majoritariamente, para controle social e opressão pelas forças policiais (KRISHNA, 2020).

Diante do exposto, vários questionamentos são suscitados sobre se o RF é uma tecnologia adequada a espaços democráticos diante da iminente possibilidade de violações de direitos fundamentais. Sendo possível a implementação de RF no âmbito da segurança pública, surge um debate sobre as maneiras de regular o RF de forma a ser uma tecnologia útil e que sua implementação esteja direcionada para a proteção de dados pessoais dos titulares que cometeram crimes ou não.

Neste artigo, estudou-se o tratamento de imagem de câmeras com tecnologia de RF em tempo real para fins de identificação de pessoas envolvidas em investigações criminais e instruções processuais penais.[4] Isso se diferencia do uso do sistema de RF para finalidade de identificação de uma pessoa por meio de imagem ou vídeo gravado, que não é verificado de forma instantânea, ou seja, em tempo real. A fim de analisar criticamente a aplicação dos princípios de proteção de dados e mapear os riscos diante do uso de tecnologia de RF, utilizou-se metodologia de revisão bibliográfica nacional e internacional sobre os desafios da tecnologia no âmbito criminal já apresentados nas escassas informações divulgadas sobre o assunto no Brasil. Assim, este artigo limitou-se a analisar os princípios da finalidade, da necessidade e da

3 *CCTV, cujo significado é* Closed Circuit Television*, é um sistema de câmeras no qual os sinais não são distribuídos publicamente, mas são monitorados, principalmente para fins de vigilância e segurança. As câmeras de CCTV recebem a designação "circuito fechado", ou seja, o acesso ao seu conteúdo é limitado apenas àqueles que podem vê-lo (ROUSE, 2012).*

4 Assim, está fora do escopo deste artigo os casos de tratamento posterior de um vídeo ou uma foto ao acontecimento de um ilícito ou algum crime, estas situações são diferentes do uso de RF para identificação de pessoas em tempo real.

transparência, já que são basilares para a Diretiva 2016/680 da UE e são os que impactam concretamente a forma de uso do RF na segurança pública. Com isso, serão desenvolvidos estes três princípios, além dos três riscos associados a não observância dessas medidas.

SEGURANÇA PÚBLICA NO BRASIL

No Brasil, o tema da segurança pública está inserido em um cenário mais amplo e, por isso, é necessário reconhecer alguns aspectos peculiares das políticas públicas criminais e do sistema penitenciário do país. Schneider e Miranda (2020, p. 4) afirmam que o Estado brasileiro, "para executar o controle social, adota uma política de segurança pública segregacionista e preconceituosa". Com isso, pensar em formas eficientes para manutenção da segurança pública perpassa pelo problema brasileiro em que há um grupo social o qual deve ser reprimido com coerção física e policial e um outro o qual deve ser protegido. Sobre essa questão, Alessandro Baratta afirma a existência de, em regra, duas classes: a classe dominante e a subalterna. A primeira "está interessada na contenção do desvio em limites que não prejudiquem a funcionalidade do sistema econômico-social e os próprios interesses e, por conseqüência, na manutenção da própria hegemonia no processo seletivo de definição e perseguição da criminalidade" (BARATTA, 2002, p. 197). Já a classe subalterna é aquela selecionada pelos mecanismos de criminalização. Em suma, o sistema penal brasileiro é muito similar ao descrito por Baratta, em que

> o sistema das imunidades e da criminalização seletiva incide em medida correspondente sobre o estado das relações de poder entre as classes, de modo a oferecer um salvo-conduto mais ou menos amplo para as práticas ilegais dos grupos dominantes, no ataque aos direitos das classes subalternas. (BARATTA, 2002, p. 198).

Ainda, é necessário refletir que temas relacionados à segurança pública, inegavelmente, remetem às questões sobre as políticas criminais adotadas pelo governo brasileiro e ao sistema penal seletivo que vigora no país. Assim, "qualquer tecnologia pensada para melhorar a segurança pública, além de considerar aspectos técnicos, precisa atentar para as variáveis de raça que perpassarão a sua utilização" (DA SILVA; DA SILVA, 2019, p. 7). Logo, a aplicação da tecnologia de RF, vista como prioridade para muitas autoridades brasileiras, possui mais uma peculiaridade diante de um sistema criminal falho e segregacionista que passa a lidar com dados delicados dos cidadãos.

ASPECTOS TÉCNICOS DO RECONHECIMENTO FACIAL

O reconhecimento facial é o resultado do uso de um algoritmo baseado em visão computacional (*computer vision*) e aprendizado de máquinas (*machine learning*), separado em dois momentos (GOOGLE CLOUD TECH, 2018) que completam o processo de RF: o reconhecimento do rosto humano, *stricto sensu*, e a identificação da pessoa (MOBIDEV, 2019). Por meio de uma ramificação do *machine learning*, o *deep learning*, a capacidade de processamento de imagens foi desenvolvida a ponto de possibilitar o RF automatizado em tempo real (BBC EARTH LAB, 2015).

O RF é um método de identificação de pessoas por meio de rostos capturados em vídeos, fotos ou imagens coletadas em tempo real. Majoritariamente, os sistemas de RF capturam e tratam dados considerados relevantes e únicos, como a distância entre os olhos ou o formato do queixo. Assim, à medida que as pessoas se movimentam por espaços públicos que possuem câmeras de vigilância com RF,

a tecnologia isola imagens faciais e extrai dados contidos nelas. Esses dados são tratados e convertidos em representações matemáticas conhecidas como *face template*, uma assinatura facial. Essa assinatura, resultante de tratamento de uma imagem capturada em tempo real, é comparada com outras assinaturas disponíveis em uma base de dados de assinaturas faciais (EFF, 2017). Essa base de dados é uma lista de *templates* de pessoas que podem ser identificadas. No contexto da segurança pública, esse banco de dados é preenchido com assinaturas faciais de sujeitos de interesse.

O resultado do tratamento dos dados faciais é representado por uma porcentagem de características semelhantes entre as duas assinaturas, essa correspondência indica a probabilidade de a pessoa que passa por uma câmera de vigilância ser ou não uma das pessoas que possuem assinatura facial contida no banco de dados. Por isso, o resultado do tratamento de dados pela tecnologia de RF não é binário, isto é, não responde: sim, o rosto capturado corresponde ao *template* existente no banco de dados; ou não, o *template* do rosto capturado pela câmera não é similar a nenhuma das assinaturas faciais contidas no banco de dados (BBW, 2018, p. 6).

Ainda, quando a tecnologia é imprecisa na identificação da pessoa e o resultado apresentado pelo RF é incorreto, ele se classifica em (i) falsos negativos ou (ii) falsos positivos. Aqueles ocorrem quando o sistema de RF falha na correspondência entre um rosto e uma assinatura facial que, de fato, está contida em um banco de dados. Ou seja, o sistema retornará erroneamente zero resultados em resposta a uma consulta, sendo que existe um resultado válido. Já um falso positivo ocorre quando o sistema reconhece a compatibilidade entre o *template* de uma pessoa capturada em tempo real e um *template* contido no banco de dados, mas a pessoa que passou pela câmera de vigilância não é quem o sistema diz que ela é (EFF, 2017).

É relevante notar que a existência de falsos negativos e falsos positivos possui consequências relevantes para aplicação na segurança pública. Por exemplo, no uso de RF, a incidência de falsos positivos causam danos às pessoas não culpáveis, visto que a identificação errônea de um inocente como uma pessoa que cometeu crime pode acarretar na prisão da pessoa errada e, possivelmente, na condenação de um sujeito que não cometeu nenhum crime. Não obstante, em caso de incidência de falsos negativos, o prejuízo é o da não identificação de uma pessoa que cometeu um crime.

A NATUREZA DO DADO TRATADO E A NECESSIDADE DE REGULAMENTAÇÃO

A informação tratada pelo RF é dado biométrico, isto significa que a tecnologia permite a identificação e a autenticação de pessoas baseada em um conjunto de informações únicas e específicas para cada pessoa (THALES, 2020). Nesse sentido, a informação facial é um dado personalíssimo e singular a cada pessoa, como as digitais dos dedos, a íris do olho e o DNA. De acordo com a LGPD, um dado biométrico, quando vinculado a uma pessoa natural, é um dado sensível (art. 5º, II). Com isso, a legislação destaca o tratamento de dados pessoais sensíveis, já que caso esses "sejam conhecidos e submetidos a tratamento, podem se prestar a uma potencial utilização discriminatória ou lesiva e que apresentariam maiores riscos potenciais do que outros tipos de informação" (DONEDA, 2019, p. 143).

Não é uníssona a possibilidade de uso de tecnologias de RF para a manutenção de segurança pública. Como evidenciado no exemplo de São Francisco (EUA), algumas autoridades e instituições entendem que os riscos e os possíveis prejuízos do tratamento de dados sensíveis são superiores aos benefícios trazidos

pelo RF utilizado no âmbito da segurança.[5] Não obstante, havendo a possibilidade de usar RF, devem ser tomadas algumas medidas de precaução e deve haver um marco regulatório que regulamente o uso de tecnologias aplicáveis à segurança pública.

Nessa perspectiva, o impacto do tratamento indevido de dados faciais de uma pessoa é significativo e os riscos de violação de direitos e liberdade individuais são elevados. Ainda, o mau uso dos dados, quando as finalidades do processamento estão no âmbito da segurança pública, geram efeitos mais gravosos, já que o direito penal é *ultima ratio*[6] e é prerrogativa do Estado contra atitudes extremas dos cidadãos.[7] Desse modo, salvaguardas específicas para o processamento de dados biométricos pelo Estado são fundamentais. Assim, no contexto europeu, a Diretiva 2016/680 prevê as peculiaridades a serem observadas no tratamento de dados pessoais para finalidades de segurança pública (art. 3º, 13 e art. 10º, Diretiva 2016/680).

A DIRETIVA 2016/680 DA UNIÃO EUROPEIA

Em 2016, o parlamento europeu e o conselho da UE estabeleceram a Diretiva 2016/680 para regulamentar a proteção das pessoas físicas no que diz respeito ao tratamento de dados pessoais pelas autoridades para efeitos de segurança pública. A diretiva explicita os princípios orientadores do tratamento de dados, como o princípio da segurança e integridade da informação, da qualidade dos dados, da finalidade, da necessidade e da transparência (art. 4º, nº 1). Estes três últimos serão tratados de forma mais específica neste artigo porque interferem diretamente no modo de uso do RF no âmbito da segurança pública, devem ser respeitados por serem princípios de proteção de dados elencados na LGPD e a observância deles está diretamente ligada com a garantia dos direitos fundamentais. Em suma, a Diretiva 2016/680 da UE busca assegurar o tratamento de informações pessoais para fins de segurança pública de forma responsável diante da proteção de dados.

PRINCÍPIO DA FINALIDADE

Um dos princípios norteadores da diretiva é o princípio da finalidade (art. 4º, 1, b).[8] Este determina que a coleta de dados pessoais deve ser feita para atingir finalidades determinadas, explícitas e legítimas diante do escopo da segurança pública. Em suma, as finalidades de tratamento de dados pessoais autorizadas pela diretiva para se atingir a segurança pública são: prevenção, investigação, deteção ou repressão de infrações penais ou execução de sanções penais, incluindo a salvaguarda e a prevenção de ameaças à segurança pública (art. 1º, nº 1).

5 *Destaca-se o* The Board of Supervisors de São Francisco *(EUA), a organização britânica* Big Brother Watch *e a Rede de Observatórios da Segurança. Ainda, algumas pesquisas usadas como referências bibliográficas para este estudo apontam para os riscos iminentes do uso indiscriminado do reconhecimento facial na área da segurança pública para a liberdade dos cidadãos.*

6 *A área penal "deve ser a* ultima ratio *do sistema normativo, isto é, deve atuar somente quando os demais ramos do Direito revelarem-se incapazes de dar a tutela devida aos bens relevantes na vida do indivíduo e da própria sociedade." (BITENCOURT, 2019, p. 58). Por isso, o tratamento de dados no âmbito da segurança pública também deve ser visto como excepcional.*

7 *A característica de* ultima ratio *está em conformidade com o princípio da intervenção mínima, isso quer dizer que o direito penal possui aspecto de responsabilização subsidiário, ele apenas existe nos ambientes em que os outros meios de controle social (civil e administrativo) não são suficientes para penalizar o sujeito. Então, adota-se medidas excepcionais.*

8 *O Considerando 29 da Diretiva 2016/680 afirma que "os dados pessoais deverão ser recolhidos para finalidades determinadas, explícitas e legítimas abrangidas pelo âmbito de aplicação da diretiva e não deverão ser tratados para fins incompatíveis com os da prevenção, investigação, deteção e repressão de infrações penais ou execução de sanções penais".*

Assim, as informações pessoais coletadas por câmeras de vigilância para manutenção da segurança pública não poderão ser utilizadas para qualquer outro fim. Ou seja, se a motivação para o uso da tecnologia é segurança pública, o instrumento ou os dados coletados por ele não poderão ser utilizados para outra finalidade. Alguns exemplos do uso de câmeras em espaços públicos que não visam a segurança são: o mapeamento de regiões populosas, a análise de horários em que o trânsito está sobrecarregado ou o rastreamento de ônibus para informar aos passageiros que a linha está atrasada. A coleta de dados para os fins anteriormente citados não estão em conformidade com a segurança pública, com isso, não é possível processar essas informações, ainda mais em caso de dados sensíveis no contexto de RF autonomizado e em tempo real. Além disso, o caminho inverso também é verdadeiro, os dados coletados para fins de segurança não podem ser tratados para outras finalidades.

Com isso, nota-se que o princípio da finalidade é balizador de algumas práticas no uso do RF para segurança pública, uma delas versa sobre a finalidade do armazenamento de dados. Para efetivação do RF, é necessário coletar informações das pessoas que se movimentam em espaços públicos para que essas sejam comparadas com *templates* de um banco de dados. Nesse sentido, são suscitados alguns questionamentos sobre a necessidade de armazenamento e retenção dos dados de todas as pessoas que circulam no local e, por isso, têm seus dados coletados, inclusive daquelas que não cometeram crimes.

Em um estudo sobre o impacto do RF no Reino Unido, o *Information Commissioner's Office* (ICO), órgão inglês para defensa dos direitos à informação, afirma que os dados pessoais processados para qualquer uma das finalidades de aplicação da lei, a exemplo do tratamento para segurança pública, devem ser mantidos por não mais do que o necessário para atingir a finalidade do processamento (ICO, 2019, p. 29). Consequentemente, torna-se necessário identificar o período de tempo em que forças policiais devem armazenar dados das pessoas que passaram por um determinado local.

Sobre essa questão, o ICO analisou dois casos de uso de RF por duas organizações policiais diferentes, a Metropolitan Police Service (MPS) e a South Wales Police (SWP). Ambas deletaram os registros resultantes do uso da tecnologia de RF após o processamento, exceto nos casos em que o sistema encontrou correspondência entre o rosto analisado instantaneamente e os *templates* contidos no banco de dados da polícia. No caso da SWP, foram excluídos todos os registros no final da implantação do RF, incluindo a imagem das pessoas reconhecidas, a imagem dos falsos positivos e, ainda, os dados da lista de observação. Já a MPS manteve registros por 30 dias, incluindo falsos positivos (ICO, 2019, p. 29). Esse cuidado de excluir os dados não usados evidencia que o interesse para a segurança pública em manter imagens ou *templates* de pessoas identificadas ou não como sujeitos de interesse é injustificável e desproporcional.

Por fim, nota-se que nem todo uso de RF é autorizado para atender a qualquer finalidade específica que vise alcançar a segurança pública. Por exemplo, o fim de preservar a segurança não é alcançado quando o RF é usado para determinar a dosimetria de pena a um indivíduo no sistema de justiça criminal (BUOLAMWINI; GEBRU, 2018, p. 1). Finalidades similares à segurança são atingidas apenas para identificar pessoas que estão na lista de interesse da polícia e que poderão enfrentar um processo judicial segundo o devido processo legal.

PRINCÍPIO DA NECESSIDADE

Para efetivação do princípio da necessidade, preza-se pela limitação do tratamento ao mínimo necessário para a realização de suas finalidades (GOV.BR, 2020, p. 14). Para adequada utilização de dados biométricos

na manutenção da segurança pública, é fundamental a observância do ciclo de vida do dado pessoal. Em regra, este possui cinco fases: coleta, retenção, processamento, compartilhamento e eliminação (GOV.BR, 2020, p. 41). Todas essas fases merecem cuidado específico no uso da tecnologia de RF. Em conformidade com o ciclo e o princípio da necessidade, frisa-se a relevância da fase de eliminação do dado. E regra, os dados devem ser processados até servirem à finalidade específica para a qual foram coletados, e quando não forem mais necessários devem ser excluídos.

Segundo o ICO (2019, p. 29), os dados processados para fins de aplicação da lei devem estar sujeitos aos cronogramas de retenção, ser revisados periodicamente e excluídos quando não for mais necessário mantê-los.[9] A necessidade de exclusão das informações pessoais é reconhecida também pela diretiva da UE, esta determina que deve-se prever "prazos adequados para o apagamento dos dados pessoais ou para a avaliação periódica da necessidade de os conservar" (art. 5º, Diretiva 2016/680).

Além disso, o Grupo de Trabalho do Artigo 29º para a proteção de dados (Article 29), grupo europeu independente que lidou com as questões relacionadas à proteção de dados e à privacidade antes da aplicação do GDPR, emitiu parecer sobre a Diretiva 2016/680. Nele, afirma-se que deve haver previsão de "critérios claros e transparentes para a avaliação da necessidade de conservar [...] dados pessoais, bem como de requisitos processuais, [...] com vista a evitar eventuais abusos" (ARTICLE 29, 2017, p. 4).

Como consequência, compreende-se que manter o *template* do rosto de uma pessoa que cometeu crime só é relevante para fins de reconhecimento facial até o momento em que essa pessoa está cumprindo sanção penal, já que após esse período, armazenar o *template* não é mais útil ou necessário e o risco de vazamento, compartilhamento ou uso indevido do dado é alto. Nesse sentido, o Article 29 (2017, p. 6) propõe um sistema de exclusão automática das informações pessoais quando o período máximo de conservação expirar e de avaliação periódica para atender a proteção de dados desde a conceção e o princípio da necessidade.

PRINCÍPIO DA TRANSPARÊNCIA

O princípio da transparência, conhecido também como princípio da publicidade, é uma das formas de combater o uso abusivo de informações e de permitir prestação de contas (*accountability*) aos titulares na construção de bancos de dados (MENDES, 2014, p. 71). Nesse sentido, a aplicação desse princípio no contexto de uso do RF para segurança pública implica a determinação de alguns parâmetros para atuação policial. Com isso, as questões que serão analisadas neste artigo são: (i) qual o banco de dados está sendo explorado pela polícia; (ii) o que o responsável pelo tratamento deve informar e registrar; e (iii) qual a necessidade de desenvolvimento de um relatório de impacto pela uso da tecnologia de RF.

Um dos pontos mais controversos é sobre a definição de qual banco de dados deve ser explorado e utilizado como referência para comparação de *templates* faciais. Questiona-se se o banco de dados adequado é o formado por todos os procurados pela polícia ou apenas por sujeitos que cometeram crimes mais graves, ainda questiona-se se os não condenados deveriam compor esse banco para RF. A extensão desse banco de dados e como ele é constituído produz inferências relevantes para os direitos de

9 *Ainda que o tratamento de dados pessoais com técnicas de reconhecimento facial para fins de prevenção de crimes não seja escopo deste artigo, a questão de saber se certos dados cumpriram seus objetivos e não são mais necessários surge quando o armazenamento de dados é permitido para fim preventivo, em que deve haver uma avaliação de risco relativa desse tratamento.*

privacidade e proteção de dados. Primeiramente, se o *template* de uma pessoa não está contido no banco de dados da polícia, ela não poderá ser reconhecida mesmo que passe na rua e tenha seus dados faciais tratados, visto que não haverá correspondência entre o seu rosto e os *templates* do banco de dados.

Portanto, um dos pontos-chave para o bom funcionamento do RF é a composição da lista de sujeitos de interesse (banco de dados ou *watchlist*) formada pelo *template* biométrico dessas pessoas. No Reino Unido, as pessoas que compõem esse banco de dados são aquelas detidas pela polícia. Nesse país, a Seção 64A da Lei de Polícia e Evidência Penal de 1984 (PACE) fornece à polícia o poder de tirar fotografias faciais de quem é detido após a prisão, chamadas de imagens de custódia. Com isso, as forças policiais podem fazer *upload* de imagens de custódia dos sistemas locais para o banco de dados nacional da polícia, o *Police National Database*.

No entanto, usar as imagens de custódia como banco de dados para o RF é complexo, já que uma grande parte das pessoas que são presas e têm uma imagem de custódia obtida nunca é acusada ou condenada por nenhum crime. No caso do Reino Unido, a organização *Big Brother Watch* (BBW) afirma que as forças policiais locais não sabem determinar quantas pessoas estão na base de dados de imagens de custódia mas são inocentes (BBW, 2018, p. 4). Por isso, a regulação brasileira para uso de tecnologias na segurança pública deve se atentar a dois pontos. Primeiro, deve ser determinado um procedimento para que a pessoa que suspeita ter sua imagem mantida ilegalmente no banco de dados da polícia possa solicitar a exclusão da imagem ou do *template*. Segundo, deve haver mecanismos que possibilitem a exclusão automática dos dados pessoais quando a pessoa que teve seus dados tratados não for acusada ou condenada por nenhum crime.

Segundo a ICO (2019, p. 17), as organizações policiais devem garantir que os dados constantes no banco de dados não sejam excessivos e que sejam utilizados somente quando estritamente necessário. Assim, nota-se que as salvaguardas da proteção de dados e dos direitos humanos apenas são cumpridas quando as forças policiais formam cuidadosamente a lista de sujeitos de interesse. Ou seja, buscam minimizar o número de pessoas em cada banco de dados e a quantidade de informações pessoais de cada pessoa e asseguram que a inclusão de novas pessoas seja feita com base no necessário para atender às finalidades do tratamento de dados.

No Brasil, a situação do sistema penal é peculiar pois há poucas informações sobre o funcionamento da burocracia penal. Por exemplo, até 2018, o número de presos apenas era estimado e o juiz de direito era pouco informado sobre a custódia do preso (CNJ, 2018, p. 9). Ainda, a superlotação dos presídios é uma realidade em todo o país: em 2019, existiam 441.147 vagas ocupadas por 733.460 pessoas (CNMP, 2020). Ainda nesse sentido, "em 2016, o Supremo Tribunal Federal declarou o estado de coisas inconstitucional em que estava o sistema penitenciário e determinou providências administrativas" (CNJ, 2018, p. 9) e, no julgamento do Recurso Extraordinário Nº 641.320/RS, foi indicado a criação de um cadastro nacional de presos pelo Conselho Nacional da Justiça.[10]

Dessa forma, o CNJ estabeleceu o Banco Nacional de Monitoramento de Prisões, em que "toda pessoa que passar pelo sistema prisional será cadastrada no Banco e ganhará um registro nacional chamado RJI (Registro Judicial Individual)" (CNJ, 2018, p. 22). Esse cadastro compila dados pessoais do preso, como fotografia, cópia de documentos e outros dados gerais. No contexto de implementação de RF, esse banco de dados se

10 *No entanto, ainda questiona-se sobre a necessidade e a operabilidade de um banco de dados centralizado de forma nacional, visto que o sistema penitenciário brasileiro é significante e, por isso, trata informações pessoais de milhares de pessoas que estão em prisões por toda extensão do país.*

assemelha ao modelo do Reino Unido, no qual, a fim de reconhecer o indivíduo que passa por câmeras de vigilância, essa pessoa tem seu *template* comparado com o de uma pessoa que teve prisão determinada.

Não obstante a necessidade de medidas que assegurem a proteção de dados aos cidadãos e a transparência no uso da tecnologia, essa não foi a realidade do caso de uso de câmeras com RF no carnaval de 2019 do Rio de Janeiro. Neste exemplo, as imagens coletadas em 28 câmeras espalhadas por Copacabana foram compiladas e transmitidas para o Centro Integrado de Comando e Controle, onde houve a comparação dos *templates* faciais com o banco de dados da Polícia Civil e do Detran (VETTORAZZO; PITOMBO, 2019). Este órgão possui informações fotográficas de todos os condutores de veículos do Estado, inclusive de pessoas inocentes e que poderiam ter sido reconhecidas mesmo sem serem sujeitos procurados pela polícia.

Quanto ao que deve ser informado e registrado pelo responsável do tratamento de dados, a Diretiva 2016/680, em seu art. 13º, assegura que informe-se ao titular alguns comunicados. O sujeito de dados deve saber sobre a finalidade do tratamento a que os dados pessoais se destinam e sobre o direito de solicitar a retificação de um dado pessoal que esteja incorreto. Ainda, para que haja transparência no processamento de dados, cabe ao responsável informar o fundamento jurídico do tratamento e o prazo de conservação dos dados ou, no mínimo, os critérios para definição desse período e os possíveis destinatários desses dados (art. 13º, nº 2). Logo, busca-se nitidez na relação entre o titular e o responsável pelo tratamento.

Além disso, o princípio da transparência é efetivado também por meio do desenvolvimento de um relatório de impacto do uso da tecnologia no âmbito da segurança pública. A diretiva europeia prevê essa avaliação, o *Data Protection Impact Assessment*. Ela indica que deve-se descrever as operações no tratamento dos dados pessoais e apresentar (i) os riscos para os direitos e para as liberdades dos titulares dos dados; (ii) as medidas previstas para fazer face a esses riscos; (iii) as garantias dos sujeitos previstas em lei; (iv) as medidas de segurança; e (v) os mecanismos para assegurar a proteção dos dados pessoais (art. 27º). Esse relatório é fundamental para que se avalie o impacto que qualquer processamento de alto risco terá sobre indivíduos e, mais importante, como especificamente buscar-se-á minimizar esses riscos. Ainda, esse documento é essencial para as forças policiais demonstrarem que o uso do RF está sobre o estritamente necessário e que os requisitos e os princípios da proteção de dados estão sendo atendidos (ICO, 2019, p. 23).

Diante do exposto, nota-se que a diretiva europeia prevê uma nova arquitetura de direitos aos titulares de dados e de atividades a serem cumpridas pelas autoridades estatais por conta do uso de novas tecnologias para efeitos de segurança pública. Assim, para que haja proteção aos dados dos titulares de forma similar ao exemplo europeu, recomenda-se que o processamento de dados sensíveis seja previsto e regulado em lei.

OS RISCOS DO RF

O uso do RF para finalidades que visem a garantia da segurança pública apresenta riscos para os direitos fundamentais do indivíduo, como a liberdade, a privacidade, a inviolabilidade da vida íntima, dentre outros aspectos. Esses riscos apontam para a possibilidade de violação de valores muito caros à sociedade moderna, a exemplo do direito de ir e vir e da garantia de igualdade entre os cidadãos. Para algumas autoridades estatais, como as da cidade de São Francisco (EUA), os riscos da tecnologia são maiores que os benefícios (CONGER; FAUSSET; KOVALESKI, 2019). Logo, é relevante pontuar essas possíveis ameaças

para que sejam implementados mecanismos efetivos de mitigação desses riscos e de proteção de dados pessoais, ainda mais quando os objetos de tratamento são dados biométricos. Por isso, dentre vários riscos, analisou-se os riscos do RF que estão ligados com a não concretização dos princípios de finalidade e necessidade, que geram (i) vigilância massiva, e de transparência, que podem acarretar em (ii) erros de acurácia e (iii) existência de viés no algoritmo.

OCORRÊNCIA DE VIGILÂNCIA MASSIVA

Em uma sociedade da informação, as pessoas constantemente informam seus dados e registram suas atividades em redes sociais e em plataformas de serviços como Netflix, Google Maps e Whatsapp. Por isso, algumas empresas possuem informações pessoais de milhares de usuários ao redor do mundo e, com o cruzamento de dados, é possível identificar padrões comportamentais e áreas de interesses individuais. Esse movimento também ocorre no setor público, em que o Estado processa dados dos cidadãos para diversas finalidades; uma delas é para a manutenção da segurança pública.

Assim, sob o fundamento de garantir segurança, "instituições governamentais armazenam e analisam dados, [...] gerenciando populações inteiras. Esta nova estruturação digital trouxe consigo a possibilidade de armazenar uma quantidade inimaginável de dados" (SCHNEIDER; MIRANDA, 2020, p. 6). Frisa-se que as consequências de tratamento de dados pessoais para segurança pública são de alto risco e podem acarretar na vigilância de toda uma população e, ainda, na prisão de pessoas. O uso indiscriminado do RF em câmeras no espaço público permite o estabelecimento de uma vigilância massiva em que o Estado é informado sobre o local o qual as pessoas frequentam, o tempo que passam em cada espaço e com quem se relacionam.

Nesse sentido, Bigo (2006, p. 47) percebeu a existência de um sistema de vigilância no contexto pós 11 de setembro, em que se criou a sensação de ameaça à segurança constante; o autor chamou esse conceito teórico de *ban-opticon*. Quando esse sistema utiliza instrumentos tecnológicos e é amplamente aplicado, se torna uma nova versão do conceito de panóptico de Foucault. Assim, "fundando-se em [...] dados biométricos e técnicas digitais de reconhecimento facial, o banóptico é capaz de realizar o controle social por intermédio da identificação preventiva de indivíduos" (SCHNEIDER; MIRANDA, 2020, p. 6). Dessa forma, há uma preocupação do uso do RF trazer demasiada vigilância a ponto de subtrair as liberdades individuais.

O uso descontrolado de RF possibilita que as forças policiais identifiquem todas as pessoas que transitam em espaços públicos, como em marchas, eventos religiosos públicos, reuniões políticas, protestos ou manifestações públicas. Além disso, com o desenvolvimento da tecnologia, esses dados podem facilmente ser cruzados com outras informações pessoais presentes na internet (PRIVACY INTERNATIONAL, 2019). A exemplo: as pessoas que se relacionam com aquela identificada em redes sociais, os registros de saúde, as informações presentes nos bancos de dados de proteção ao crédito, o endereço de residência ou as preferências sexuais. Para ilustrar, os manifestantes que participaram dos protestos de Hong Kong em 2019 tiveram a preocupação de evitar que câmeras de RF funcionassem naquele contexto por meio do uso de laser, visto que isso permitiria identificação das pessoas no contexto político (TREVISAN, 2019).

Com a permanente vigilância e supervisão do Estado sob o pretexto de segurança, cria-se uma condição em que parte da liberdade das pessoas encontra-se ferida. Não há mais ampla autonomia

para desenvolvimento da personalidade e para autodeterminar-se, visto que as pessoas estão sendo constantemente observadas. Além disso, os direitos de privacidade e inviolabilidade da intimidade, mesmo que exercidos em espaços públicos, são violados e, por isso, constrói-se um entendimento de que os dados pessoais, como as informações biométricas de uma pessoa, não estão mais sob os poderes do sujeito de dados, mas sob o controle do Estado, que decide livremente a forma de tratar essas informações.

Além disso, a vigilância exercida pelo uso da RF é potencializada, visto que é possível identificar uma pessoa independente de contato físico ou autorização prévia. Anteriormente, a pessoa identificada tinha conhecimento de estar sendo identificada e da finalidade à qual aquele dado estava sendo usado, como em pontos de fiscalização no trânsito ou na migração em um país. Porém, com o RF, é possível saber onde a pessoa se encontra sem ela saber que está sendo observada. Dessa forma, cada vez mais as pessoas estão sujeitas ao tratamento de dados biométricos e às verificações de identidade sem nem sequer estarem cientes disso. A falta de regulação e de determinação de uma finalidade específica para uso da tecnologia e o uso indevido de câmeras criam um estado de vigilância massiva.

Diante da falta de regulação, o ICO (2019, p. 3) evidencia os riscos do uso da tecnologia de RF para fins de segurança: o potencial de permitir a vigilância em larga escala e o impacto que isso tem sobre os direitos humanos e os direitos de informação das pessoas. O BBW (2018, p. 13) aponta que o uso indiscriminado de RF é uma ameaça à privacidade, porquanto câmeras com RF podem atuar como postos de controle para identificação biométrica. Esse tipo de uso da tecnologia não visa à manutenção da segurança pública, já que coleta informações não necessariamente úteis. Ainda, mesmo que a coleta fosse apenas de pessoas que cometeram crimes, é fundamental observar as devidas formas de tratamento em respeito à proteção de dados. A liberdade de expressão e o direito de realizar atividades diárias sem perturbações de autoridades estatais, ir aonde quiser e com quem quiser, e participar de eventos e manifestações são mitigados quando o uso de RF não é regulamentado (BBW, 2018, p. 13).

Quanto à vigilância massiva, a China desenvolveu um sistema próprio de classificação dos cidadãos, o *Social Credit System* (SCS), que possibilita a integração de sistemas de crédito, punição, recompensa e identidade do indivíduo. Em suma, os indivíduos são rastreados por câmeras de vigilância e são classificados em quatro áreas: atividades comerciais, comportamentos sociais, interesse administrativo e cumprimento das leis (MAURTVEDT, 2017, p. 16). Com isso, por meio dessas notas, consequências são aplicadas aos cidadãos, por exemplo, mais de nove milhões de chineses com notas baixas nesse sistema não puderam comprar passagens em voos domésticos (MA, 2018). Especificamente sobre o RF, a China está desenvolvendo mecanismos que comparam, de forma automática e instantânea, rostos com mais de 1,3 bilhões de fotos de identificação em segundos para auxiliar o rastreamento dos cidadãos (JIAQUAN, 2018). Ainda, o site do SCS já encoraja os cidadãos a informarem seus dados faciais para o sistema por meio de fotos do rosto, sendo assim, mais uma informação seria incorporada ao grande banco de dados chinês (MATSAKIS, 2019).

A inexistência de um regulamento para proteger a privacidade dos cidadãos é uma das razões pela qual a China talvez tenha a maior quantidade de dados pessoais disponíveis e a mais avançada tecnologia em inteligência artificial habilitada para vigilância (MAURTVEDT, 2017, p. 19). Nesse sentido, o SCS reforça os princípios e os fundamentos da vigilância, induzindo os cidadãos chineses a um estado de vigilância permanente que garante a execução das funções do poder. No caso chinês, o poder detido pelo Estado é derivado da capacidade não juridicamente regulada de tratar informações e extrair conhecimentos de dados sobre os sujeitos, e, ainda, da possibilidade de restringir o acesso aos bens e serviços comuns (MAURTVEDT, 2017, p. 50).

ERROS DE ACURÁCIA

Outro problema no uso da tecnologia de RF é o nível de inacurácia do sistema, ou seja, a porcentagem de vezes em que o RF falha, seja quando identifica uma pessoa errada ou não identifica sujeitos que eram procurados. Nota-se que um sistema com baixa acurácia produz resultados prejudiciais à população, ainda mais quando o uso dos dados está no âmbito da segurança.

Um relatório do BBW (2018, p. 3) indica que, no Reino Unido, 95% de correspondências feitas por RF resultaram em identificação incorreta de pessoas inocentes. Ou seja, do total de pessoas reconhecidas pelo sistema como um *template* contido na base de dados, 95% eram falsos positivos. A incidência da baixa acurácia gera efeitos na atuação policial quanto às questões sobre o princípio da finalidade e necessidade de armazenamento de fotos das pessoas. Diante da alta porcentagem de inacurácia, mesmo que as forças policiais apaguem todas as imagens que não tiveram correspondência no uso de RF, armazenar as fotos de todas as pessoas que correspondiam com banco de dados não é suficiente para proteção de dados. Nesse caso, 95% das fotos mantidas pela polícia não estariam atendendo à finalidade da segurança pública, visto que os índices de erro do sistema são elevados.

No Rio de Janeiro em 2019, uma mulher inocente foi confundida pelo sistema de RF com uma mulher que cometeu crimes; ela teve de ser conduzida à delegacia e só depois foi liberada. Neste caso, ainda um erro na formação do banco de dados da polícia foi evidenciado, pois a mulher que realmente estava sendo procurada já estava presa desde 2015, mas mesmo assim constava na lista de sujeitos de interesse da polícia (CORREIO, 2019). Com isso, a inacurácia do sistema é um erro que precisa ser endereçado.

Para evitar as consequências da inacurácia, é argumentado que a pessoa a qual verifica a correspondência entre a face e o *template*, majoritariamente policiais, poderia ser treinada para compreender o sistema de RF em uso e perceber quando deve-se abordar a pessoa potencialmente identificada. No entanto, existem no mínimo dois impasses: na maioria das vezes, os templates do banco de dados não estão associados à fotografia da pessoa procurada, mas apenas à representação matemática da foto; e as forças policiais não possuem um treinamento especializado para tomarem melhores decisões com o RF (EFF, 2017). O ICO (2019, p. 31) frisa a necessidade de revisão de políticas de privacidade, práticas de governança, procedimentos e treinamentos da atuação policial, além da necessidade de práticas de avaliação de risco à proteção de dados pessoais tendo em vista o uso de novas tecnologias.

Sobre aspectos técnicos, algumas características da imagem podem atrapalhar no bom funcionamento do RF, as principais são: iluminação, enquadramento do rosto, expressão facial, qualidade de imagem e envelhecimento facial. Além disso, alguns estudos apontam que grupos demográficos específicos de etnia, gênero e idade são mais susceptíveis a sofrerem erros no processo de RF (BUOLAMWINI; GEBRU, 2018, p. 1).

EXISTÊNCIA DE VIÉS NO ALGORITMO

As entidades que lidam com RF sinalizam os aspectos discriminatórios na forma de concepção da tecnologia. O desempenho dos algoritmos de RF são prejudicados se os dados utilizados para treinamento da tecnologia, os *templates* faciais, não forem representativos (KLARE *et al.*, 2012, p. 1791). O ICO (2019, p. 33) pontua que o sistema pode possuir viés se as faces que foram utilizadas no treinamento do algoritmo não tiverem uma representatividade equilibrada da população, ou seja, se as variações de cor e etnia não

forem observadas. Logo, a taxa de precisão e acurácia será diferente para rostos que o sistema não foi treinado e, por isso, não está familiarizado.

Foi realizado um estudo com diferentes algoritmos de classificação de gênero, idade e etnia diante de rostos para analisar se os algoritmos de RF exibem vieses demográficos quando utilizados em grupos específicos (KLARE *et al.*, 2012, p. 1789). Notou-se variações para pior no desempenho do RF quando exposto a grupos demográficos representativos, isto é, com grande presença de pessoas variadas, como mulheres, negros e jovens. Após a avaliação dos diferentes algoritmos de classificação pelo rosto, confirmou-se que eles não apenas apresentam desempenho significativamente pior em certos cortes demográficos, como consistentemente apresentam pior performance nos mesmos grupos, sempre entre mulheres, negros e indivíduos mais jovens, entre 18 e 31 anos (KLARE *et al.*, 2012, p. 1789).

Portanto, treinar sistemas de RF em banco de dados demograficamente bem distribuídos é fundamental para reduzir a vulnerabilidade de certos grupos sociais diante de taxas de inacurácia elevada se comparada à tentativa de reconhecer pessoas em um grupo de homens brancos. Outra conclusão é que o desempenho do RF em grupos étnicos e de idade específicos melhora quando o sistema é treinado exclusivamente para esse grupo demográfico (KLARE *et al.*, 2012, p. 1800).

Da perspectiva do reconhecimento facial automatizado, o teste realizado pelo *National Institute of Standards and Technology* (NIST), agência governamental estadunidense sobre inovação e competitividade tecnológica, (2019, p. 7) apontou que os algoritmos de RF têm variações na acurácia dependendo do grupo demográfico de um sujeito. Entre outras descobertas, este estudo demonstrou que os falsos positivos são entre 2 e 5 vezes maiores em mulheres que em homens, variando de acordo com o algoritmo, país de origem e idade (NIST, 2019, p. 7). Este aumento está presente para a maioria dos algoritmos e conjunto de dados (*datasets*) testados pelo NIST. Ainda, a menor taxa de falso positivo ocorre com indivíduos europeus (NIST, 2019, p. 7), que são majoritariamente brancos.

Ainda, uma pesquisa conduzida pelo *Massachusetts Institute of Technology* (MIT) aponta que algoritmos comercializados para a fase de reconhecimento de rostos erram em classificar mulheres negras em até 34,7%, e homens brancos em, no máximo, 0,8% (BUOLAMWINI; GEBRU, 2018, p. 1). A performance de algoritmos de classificação de gênero foi melhor em pessoas com cor de pele mais clara. Com exemplo, a taxa de erro de algoritmos da Microsoft foi de 12,9% em pessoas de pele negra e 0,7% em pessoas de pele clara, já algoritmos da IBM tiveram taxas de erro superiores a 22% em pessoas de pele negra (BUOLAMWINI; GEBRU, 2018, p. 10).

A principal explicação para a atuação diferente do RF em relação à cor de pele está no processo de treinamento do algoritmo de RF. Será mais fácil de reconhecer alguém do grupo de faces em que um algoritmo é treinado, pois ele possui familiaridade com os atributos faciais daquele grupo. Porém, quando esses grupos de rostos representam uma etnia de forma desproporcional, um algoritmo otimiza sua precisão para esse grupo em detrimento de outros (GARVIE; BEDOYA; FRANKLE, 2016). Portanto, as pesquisas evidenciam menor acurácia quando o RF é usado para identificar uma diversidade maior de pessoas, especificamente mulheres negras, visto que possuem atributos faciais distintos de homens brancos. Diante disso, é fundamental o estabelecimento de relatórios rigorosos sobre as métricas de desempenho da tecnologia para que haja transparência no funcionamento do algoritmo e possa haver debates sobre o uso ético do RF.

O tópico da discriminação, diante da existência de viés no algoritmo, ligada ao uso do RF é ainda mais sensível quando a tecnologia é usada para auxiliar a segurança pública de um país com diversas etnias

e com um sistema penal racista. Um grupo demográfico sub-representado no conjunto de dados de referência do algoritmo de RF pode estar sujeito à identificação errônea frequente. Assim, é fundamental analisar as consequências do aumento da representação fenotípica e demográfica em conjuntos de dados faciais e na avaliação algorítmica.

CONCLUSÃO

Em suma, a atuação policial e o uso de novas tecnologias no âmbito do direito penal só serão legítimos e constitucionais se regulamentados em conformidade com os direitos constitucionais do devido processo legal, da privacidade e da proteção de dados do titular. Com isso, garante-se que, por mais relevante que a segurança pública, em sentido amplo, e o interesse público sejam, os direitos individuais não serão violados e não será instaurada situação de vigilância massiva e constante dos cidadãos. Nesse sentido, nota-se que a tecnologia de RF pode ser vista como instrumento conveniente, no entanto é primordial pensar nos novos desafios advindos pela utilização da tecnologia e na preservação de direitos fundamentais e de valores sociais relevantes, como a privacidade e o direito de ir e vir.

No contexto do RF, restou evidente que o uso dessa tecnologia expõe as pessoas a riscos elevados e peculiares, podendo ser identificadas mesmo sem aviso ou consentimento prévio. Esses riscos são ainda mais manifestos quando a tecnologia é utilizada para finalidades similares à segurança pública, já que essencialmente o direito penal é intrusivo, excepcional e possui papel de balizar e limitar o poder punitivo do Estado. Porém, se não houver regulamento adequado e direcionado para a proteção de dados, existe o risco iminente de a regra ser a vigilância digital, o controle e a penalização dos cidadãos. Não obstante o RF já estar sendo utilizado pelas forças policiais brasileiras, é fundamental a promulgação de uma legislação que proíba o uso da tecnologia nesse contexto ou, ao menos, que coíba o uso abusivo.

Diante do exposto, qualquer forma de regulamentação escolhida deve prever salvaguardas, especialmente sobre o princípio da finalidade, da necessidade e da transparência. O princípio da finalidade tem função específica de delinear as motivações legítimas de uso da tecnologia para aplicação na segurança e, de certa forma, minimizar a quantidade de dados coletados, armazenados e tratados pelo Estado. Quanto à necessidade, as informações pessoais devem ser atualizadas e tratadas apenas quando necessário e, quando não mais úteis, devem ser apagadas. O princípio da transparência garante que sejam assegurados os direitos dos titulares de dados, a atuação legal das forças policiais e a possibilidade de supervisão, e o controle do uso da tecnologia pela sociedade.

Como consequência, se uma lei autorizar o uso dos sistemas de RF na segurança pública, ela deve explicitar balizas de aplicação dos princípios de proteção de dados. Com isso, seria possível que a tecnologia fosse utilizada apenas para uma finalidade específica em um caso concreto determinado, nunca para atender uma motivação vaga ou imprecisa. Assim, a autoridade que utilizasse a tecnologia apenas faria tratamento de dados pessoais de pessoas de interesse por tempo em que houvesse necessidade, e nada além disso. Ainda, todo esse processo de utilização da tecnologia pelas autoridades policiais seria seguida de ampla transparência com todos os cidadãos para que pudesse haver escrutínio público sobre a proporcionalidade e a utilidade da tecnologia de reconhecimento facial.

Além disso, a observação de regulamentos específicos e da proteção de dados pessoais também tem como finalidade mitigar os riscos advindos pelo uso da tecnologia. A ameaça de concretização

desses riscos põe em perigo direitos fundamentais previstos na Constituição brasileira e a liberdade básica do indivíduo. Os três principais riscos endereçados neste artigo são: a vigilância massiva, os erros de acurácia e a existência de viés no algoritmo. A vigilância potencializada pela desregulação no uso de RF coloca todos os cidadãos em um sistema de observação em que todos são suspeitos. Isso vai de encontro com garantias fundamentais e direitos de privacidade. Diante dos riscos do RF, é fundamental garantir uma frequência dos testes de acurácia e de precisão da tecnologia por meio de testes padronizados e independentes para analisar as taxas de erro diante de tendências étnicas e de gênero. Ainda, a falta de acurácia e a existência de, em regra, bases de dados de treinamento enviesadas possuem como consequência a discriminação de grupos que são mais prováveis de serem identificados erroneamente pelo RF. Logo, tecnologias que possuem esse viés não deveriam ser utilizadas de qualquer forma pelo poder público. Este apontamento se agrava diante do sistema criminal racista do Brasil.

Portanto, as consequências do uso do RF para a segurança são reconhecidas e devem ser melhor analisadas para que se entenda a possibilidade ou não de aplicação dessa tecnologia no âmbito da segurança pública no Brasil, país que possui sistema penal falho e segregacionista. No entanto, os efeitos do RF só serão devidamente alcançados se o uso for proporcional e se houver equilíbrio entre a privacidade dos indivíduos e a aplicação da lei. Não é desejável que se escolha um tema em detrimento do outro, como a segurança pública frente às liberdades humanas que possibilitam desenvolvimento autônomo da personalidade, visto que os malefícios dessa escolha atingem os valores de uma sociedade democrática e são de difícil compensação.

REFERÊNCIAS BIBLIOGRÁFICAS

ARTICLE 29. **Parecer sobre algumas questões importantes da Diretiva relativa à proteção de dados na aplicação da lei (Diretiva [UE] 2016/680)**. 2017. Disponível em: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=610178. Acesso em: 5 maio 2020.

BARATTA, A. **Criminologia Crítica e Crítica do Direito Penal**: introdução à sociologia do direito penal. Tradução: Juarez Cirino dos Santos. 3 ed. Rio de Janeiro: Editora Revan, Instituto Carioca de Criminologia, 2002.

BBC EARTH LAB. **How Does Facial Recognition Work? | Brit Lab**. Canal do Youtube, 26 nov. 2015. Disponível em: https://www.youtube.com/watch?v=1aHub80AHFk. Acesso em: 24 jul. 2020.

BBW – Big Brother Watch. **Face Off: the lawless growth of facial recognition in UK policing**. maio 2018. Disponível em: https://bigbrotherwatch.org.uk/wp-content/uploads/2018/05/Face-Off-final-digital-1.pdf. Acesso em: 5 maio 2020.

BIGO, D. Security, Exception, Ban and Surveillance. *In:* LYON, D. **Theorizing Surveillance**. The Panopticon and beyond. Reino Unido: Wilan, 2006, p. 46-68.

BITENCOURT, C. R. **Tratado de Direito Penal**: parte geral. v. 1, 19 ed. São Paulo: Saraiva Educação, 2019.

BRASIL. **Lei Nº 13.444**, de 11 de maio de 2017. Dispõe sobre a Identificação Civil Nacional (ICN). Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2017/lei/l13444.htm. 5 maio 2021.

BUOLAMWINI, J.; GEBRU; T. Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification. **Conference on Fairness, Accountability, and Transparency**, Proceedings of Machine Learning Research, v. 81, p. 1-15, 2018.

CÂMARA DOS DEPUTADOS. Comissão de Ciência e Tecnologia, Comunicação e Informática. **Audiência Pública Ordinária 03/04/2019**. Disponível em: https://www.camara.leg.br/evento-legislativo/54893. Acesso em: 5 maio 2020.

CNJ – Conselho Nacional de Justiça. **Banco Nacional de Monitoramento de Prisões** – BNMP 2.0: Cadastro Nacional de Presos. Brasília: CNJ, ago. 2018. Disponível em: https://www.cnj.jus.br/wp-content/uploads/2018/01/57412abdb54eba909b3e1819fc4c3ef4.pdf. Acesso em: 7 maio 2020.

CNMP – Conselho Nacional do Ministério Público. **Sistema Prisional em números**. 2020. Disponível em: https://www.cnmp.mp.br/portal/relatoriosbi/sistema-prisional-em-numeros. Acesso em: 15 maio 2020.

CONGER, K.; FAUSSET, R.; KOVALESKI, S. **San Francisco Bans Facial Recognition Technology**. The New Yorl Times, 14 maio 2019. Disponível em: https://www.nytimes.com/2019/05/14/us/facial-recognition-ban-san-francisco.html. Acesso em: 5 maio 2020.

CORREIO. Inocente é confundida com criminosa por câmera de reconhecimento facial no Rio. **Correio**, Da redação, 11 jul. 2019. Disponível em: https://www.correio24horas.com.br/noticia/nid/inocente-e-confundida-com-criminosa-por-camera-de-reconhecimento-facial-no-rio/. Acesso em: 8 maio 2020.

DA SILVA, R. L.; DA SILVA, F. dos S. R. Reconhecimento facial e segurança pública: os perigos do uso da tecnologia do sistema penal seletivo brasileiro. **Anais do 5º Congresso Internacional de Direito e Contemporaneidade**: Mídias e Direitos da Sociedade em Rede. Santa Maria/RS, 2019.

DONEDA, D. **Da privacidade à proteção de dados pessoais**: elementos da formação da Lei geral de proteção de dados. 2 ed. São Paulo: Thomson Reuters Brasil, 2019.

EFF – Electronic Fontier Foudation. **Face Recognition**. 2017. Disponível em: https://www.eff.org/pages/face-recognition. Acesso em: 5 maio 2020.

GARVIE, C.; BEDOYA, A.; FRANKLE, J. The Perpetual Line-up. Unregulated police face recognition in America. **Center on Privacy & Technology at Georgetown Law**, 18 out. 2016. Disponível em: https://www.perpetuallineup.org/findings/racial-bias#footnote223_i485k1t. Acesso em: 12 maio 2020.

GOOGLE CLOUD TECH. **How Computer Vision Works**. Canal do Youtube, 19 abr. 2018 Disponível em: https://www.youtube.com/watch?v=OcycT1Jwsns&t=32s. Acesso em: 24 jul. 2020.

GOV.BR. **Guia de Boas Práticas** – Lei Geral de Proteção de Dados (LGPD). ago. 2020. Disponível em: https://www.gov.br/governodigital/pt-br/governanca-de-dados/guia-lgpd.pdf. Acesso em: 6 maio 2020.

ICO – Information Comissioner's Office. **ICO investigation into how the police use facial recognition technology in public places**. 31 out. 2019. Disponível em: https://ico.org.uk/media/about-the-ico/documents/2616185/live-frt-law-enforcement-report-20191031.pdf. Acesso: 6 maio 2020.

IPE - Instituto de Pesquisa Econômica Aplicada. **Atlas da Violência,** v. 2.7. 2019. Disponível em: https://www.ipea.gov.br/atlasviolencia/download/19/atlas-da-violencia-2019. Acesso em: 8 maio 2021.

JIAQUAN, Z. Drones, facial recognition and a social credit system: 10 ways China watches its citizens. **South China Morning Post, People & Culture**, 4 ago. 2018. Disponível em: https://www.scmp.com/news/china/society/article/2157883/drones-facial-recognition-and-social-credit-system-10-ways-china. Acesso em: 8 maio 2020.

JÚNIOR, J. Maia cria comissão de juristas para propor lei sobre uso de dados pessoais em investigações. **Portal da Câmara dos Deputados**, Notícias, 27 nov. 2019. Disponível em: https://www.camara.leg.br/noticias/618483-maia-cria-comissao-de-juristas-para-propor-lei-sobre-uso-de-dados-pessoais-em-investigacoes/. Acesso em: 25 jul. 2020.

KLARE, B. F.; BURGE, M. J.; KLONTZ, J. C.; BRUEGGE, R. W. V.; JAIN, A. K. Face Recognition Performance: Role of Demographic Information. **IEEE Transactions on Information Forensics and Security**, v. 7, n. 6, p. 1789-1801, dez. 2012.

KRISHNA, A. **IBM CEO's Letter to Congress on Racial Justice Reform**. IBM, 8 jun. 2020. Disponível em: https://www.ibm.com/blogs/policy/facial-recognition-sunset-racial-justice-reforms/. Acesso em: 5 set. 2020.

LAVADO, T. Aumento do uso de reconhecimento facial pelo poder público no Brasil levanta debate sobre limites da tecnologia. **G1**, Economia, Tecnologia, 21 fev. 2020. Disponível em: https://g1.globo.com/economia/tecnologia/noticia/2020/02/21/aumento-do-uso-de-reconhecimento-facial-pelo-poder-publico-no-brasil-levanta-debate-sobre-limites-da-tecnologia.ghtml. Acesso em: 5 maio 2020.

LISBOA, V. Câmeras de reconhecimento facial levam a prisões no carnaval do Rio. **Agência Brasil**, Rio de Janeiro, 8 mar. 2019. Disponível em: https://agenciabrasil.ebc.com.br/geral/noticia/2019-03/cameras-de-reconhecimento-facial-levam-4-prisoes-no-carnaval-do-rio. Acesso em: 5 maio 2020.

MA, A. China has started ranking citizens with a creepy 'social credit' system — here's what you can do wrong, and the embarrassing, demeaning ways they can punish you. **Business Insider**, Internationaal, 30 out. 2018. Disponível em: https://www.businessinsider.com/china-social-credit-system-punishments-and-rewards-explained-2018-4. Acesso em: 8 maio 2020.

MANN, M.; SMITH, M. Automated Facial Recognition Technology: recent developments and approaches to oversight. **UNSW Law Journal**, v. 40, n. 1, p. 121-145, 2017.

MATSAKIS, L. How the West Got China's Social Credit System Wrong. **Wired**, Security, 29 jul. 2019. Disponível em: https://www.wired.com/story/china-social-credit-score-system/. Acesso em: 8 maio 2020.

MAURTVEDT, M.. **The Chinese Social Credit System**. Surveillance and Social Manipulation: A Solution to "Moral Decay"?. Tese (Doutorado em Sociedade e Política Chinesa) – Department of Culture Studies and Oriental Languages, University of Oslo, Norway, 2017.

MENDES, L. S. **Privacidade, proteção de dados e defesa do consumidor**: linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014, cap. 1, p. 23 -78.

NIS - National Institute of Standards and Technology. **Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects**. 2019. Disponível em: https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf. Acesso em: 5 maio 2021.

METRÔ. Metrô compra sistema de monitoramento eletrônico com reconhecimento facial. **Metrô**, Notícias, 2019. Disponível em: http://www.metro.sp.gov.br/noticias/28-06-2019-metro-compra-sistema-de-monitoramento-eletronico-com-reconhecimento-facial.fss. Acesso em: 5 maio 2020.

MOBIDEV. **Face Detection & Recognition Software based on Machine Learning**. Canal do Youtube, 22 maio 2019. Disponível em: https://www.youtube.com/watch?v=X7_ojlEXnWc. Acesso em: 24 jul. 2020.

PRIVACY INTERNATIONAL. **Protecting Civic Spaces**. 1 maio 2019. Disponível em: https://privacyinternational.org/long-read/2852/protecting-civic-spaces. Acesso em: 8 maio 2020.

ROUSE, M. **CCTV (closed circuit television)**. WhatIs, TechTarget, 2012. Disponível em: https://whatis.techtarget.com/definition/CCTV-closed-circuit-television. Acesso em: 15 maio 2020.

SABBAGH, D. Facial recognition row: police gave King's Cross owner images of seven people. **The Guardian**, Technology, 4 out. 2019. Disponível em: https://www.theguardian.com/technology/2019/oct/04/facial-recognition-row-police-gave-kings-cross-owner-images-seven-people. Acesso em: 11 out. 2019.

SCHNEIDER, C. B.; MIRANDA, P. F. M. Vigilância Digital como instrumento de promoção da segurança pública. **Publicatio UEPG – Ciências Sociais Aplicadas**, Ponta Grossa/RS, v. 28, p. 1-14, 2020.

THALES. Biometrics: authentication & identification (definition, trends, use cases, laws and latest news) – 2020 Review. **Thales**, 2020. Disponível em: https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/inspired/biometrics. Acesso em: 5 maio 2020.

TREVISAN, B . Manifestantes usam laser contra câmeras de reconhecimento facial. **Olhar Digital**, Notícias, 1 ago. 2019. Disponível em: https://olhardigital.com.br/noticia/manifestantes-usam-laser-contra-cameras-de-reconhecimento-facial/88677. Acesso em: 25 jul. 2020.

UNIÃO EUROPEIA. Diretiva (UE) 2016/680 do Parlamento Europeu e do Conselho, de 27 de abril de 2016. **Jornal Oficial da União Europeia**, 4 maio 2016. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016L0680&from=EN. Acesso em: 6 maio 2020.

VETTORAZZO, L.; PITOMBO, J. P. Rio e Salvador terão sistema de reconhecimento facial no Carnaval. **Folha de S. Paulo**, Cotidiano, 27 fev. 2019. Disponível em: https://www1.folha.uol.com.br/cotidiano/2019/02/rio-e-salvador-terao-sistema-de-reconhecimento-facial-no-carnaval.shtml. Acesso em: 7 maio 2020.

REVISTA
BRASILEIRA
DE SEGURANÇA PÚBLICA