

Sorria! Você está Sendo Filmado: As Problemáticas Envolvidas no uso de Reconhecimento Facial em Cidades Inteligentes

SABRINA CALLEGARO

PONTIFÍCIA UNIVERSIDADE CATÓLICA DO RIO GRANDE DO SUL (PUCRS)

ROSIANE ALVES PALACIOS

PONTIFÍCIA UNIVERSIDADE CATÓLICA DO RIO GRANDE DO SUL (PUCRS)

KÁTIA ELOISA BERTOL

PONTIFÍCIA UNIVERSIDADE CATÓLICA DO RIO GRANDE DO SUL (PUCRS)

Agradecimento à orgão de fomento:

O presente trabalho foi realizado com o apoio da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior - Brasil (CAPES) - Código de financiamento 001.

Sorria! Você está Sendo Filmado: As Problemáticas Envolvidas no uso de Reconhecimento Facial em Cidades Inteligentes

1 INTRODUÇÃO

Já faz um tempo considerável que a sociedade busca meios de identificar os indivíduos. Diferenciar as pessoas seja pelas impressões digitais, pela íris, ou pela fisionomia, já é uma prática. O tema do reconhecimento facial (RF), há muito retratado em filmes começa a ser debatido pela academia e pela sociedade. Mais especificamente, as pesquisas sobre essa temática iniciaram na década de 1960 e, até hoje, existe forte interesse em criar mecanismos capazes de viabilizar o processamento das imagens capturadas de forma automatizada (CRIPPA, 2021). O antigo retrato falado pôde ser aprimorado pela tecnologia da informação e comunicação (TIC). Na atualidade há uma grande variedade de aplicações para o RF que vão desde a vigilância, até a interação entre máquina e corpo humano (CRIPPA, 2021). Por meio dessa ferramenta e com o uso de um banco de dados é possível reconhecer o rosto de indivíduos a partir de uma análise de dados anteriormente coletados. Na atualidade essa técnica está disponível mesmo em smartphones.

O RF tem o potencial de agregar valor e trazer benefícios tanto para a sociedade como para os indivíduos, mas pode também infringir seriamente a seara dos direitos individuais - elevando o potencial para uma sociedade de vigilância em grande escala (BUCKLEY; HUNTER, 2011). Os estudos sobre o RF estão pautados muito mais em como fazê-lo dar certo do que nos seus potenciais reflexos negativos. Embora o reconhecimento facial tenha ou venha a beneficiar a sociedade contemporânea de muitas maneiras, as controvérsias e as preocupações estão aumentando (ZENG et al, 2019). As formas pelas quais o RF é capaz de interferir nos direitos relacionados à privacidade dos cidadãos são multifacetadas e complexas (PURSHOUSE; CAMPBELL, 2019). No Brasil, por exemplo, o reconhecimento facial foi implantando nos seguintes aplicativos do governo federal: Meu GOV.BR e Meu INSS. A adoção do RF é justificada como uma forma de autenticação, sendo que este também é utilizado para prova de vida dos aposentados do Instituto Nacional do Seguro Social (INSS), por exemplo (MINISTÉRIO DA ECONOMIA, 2020).

No contexto das cidades, que com cada vez mais frequência se utilizam de câmeras de vigilância e aparatos de Internet das Coisas (IoT), essa tecnologia pode dar apoio à tomada de decisão e ser aplicada em áreas como a mobilidade e a segurança (JANSEN; MATHEUS; ZUIDERWIJK, 2015). A utilização do RF também ocorre em edifícios comerciais, metrô, shoppings centers e, entre outros, onde uma grande quantidade de usuários pode estar presente simultaneamente (RIVERO-ANGELES, 2021). Premiadas iniciativas de cidades inteligentes (CI) como o Centro de Operações do Rio da cidade do Rio de Janeiro ou o Centro Integrado de Comando (CEIC) da cidade de Porto Alegre são exemplos de cidades que utilizam câmeras para o apoio à tomada de decisão e governança (PEREIRA, *et al.* 2017). Essas iniciativas têm o potencial de coletar inúmeros dados entre eles dados de RF dos cidadãos. Na cidade de São Paulo, por exemplo, as câmeras do metrô capturavam as diferentes reações dos usuários do meio de transporte coletivo diante das propagandas nas telas multimídias, tudo sem o devido consentimento dos cidadãos, o que acabou resultando em processo judicial que suspendeu o uso desta tecnologia (COSTA, 2020).

A implantação de sistemas de RF contribui para tornar a vigilância mais efetiva nas cidades, até mesmo como uma forma de otimizar o trabalho de órgãos de segurança pública (MONTEIRO, 2021), entretanto apresenta um risco de que qualquer sucesso na prevenção do crime venha às custas dos direitos de pessoas inocentes que podem estar sujeitas a medidas de

policiamento coercivos (PURSHOUSE; CAMPBELL, 2019). Com o uso de RF, pessoas em maior situação de vulnerabilidade social podem ser ainda mais marginalizadas e estereotipadas pela sociedade.

A utilização de sistemas e mecanismos de RF impactam na redução da privacidade, pois há um tratamento massivo de dados pessoais pelos responsáveis pela coleta destes dados, considerados sensíveis sob a perspectiva da Lei Geral de Proteção aos Dados e trazendo a debate a necessidade de proteção destes dados (MONTEIRO, 2021). Apesar do uso do RF estar em ascensão, cabe ainda à sociedade realizar reflexões mais profundas acerca de sua aplicação. É necessário que se investiguem e problematizem os objetivos e consequências dessa técnica. Neste sentido, este ensaio teórico teve como objetivo discorrer sobre o uso da ferramenta de reconhecimento facial em cidades a fim de problematizar oportunidades e ameaças para as cidades inteligentes. No Brasil e no mundo, ainda não há consenso sobre como deve ser a regulamentação de tal tecnologia. Há aqueles que temem seus potenciais, pois pode configurar ferramenta para monitoramento abusivo e os que reconhecem potenciais benefícios para a sociedade.

2 EXPERIÊNCIAS DE RECONHECIMENTO FACIAL NO BRASIL

Um mapeamento da Surfshark, empresa que desenvolve ferramentas de proteção de privacidade na internet, revela que 98 países usam tecnologias de reconhecimento facial em algum tipo de vigilância pública, conforme levantamento divulgado em maio de 2020, que considerou dados de 194 países e apontou que, além dos que já utilizam, 12 aprovavam, mas ainda não implementaram esse tipo de tecnologia; 13 consideravam aplicá-la; 68 não utilizavam e três proibiam (MARASCIULO, 2020). Conforme esse mapeamento, 92% dos países na América do Sul usam reconhecimento facial, a maior porcentagem entre os continentes (MARASCIULO, 2020).

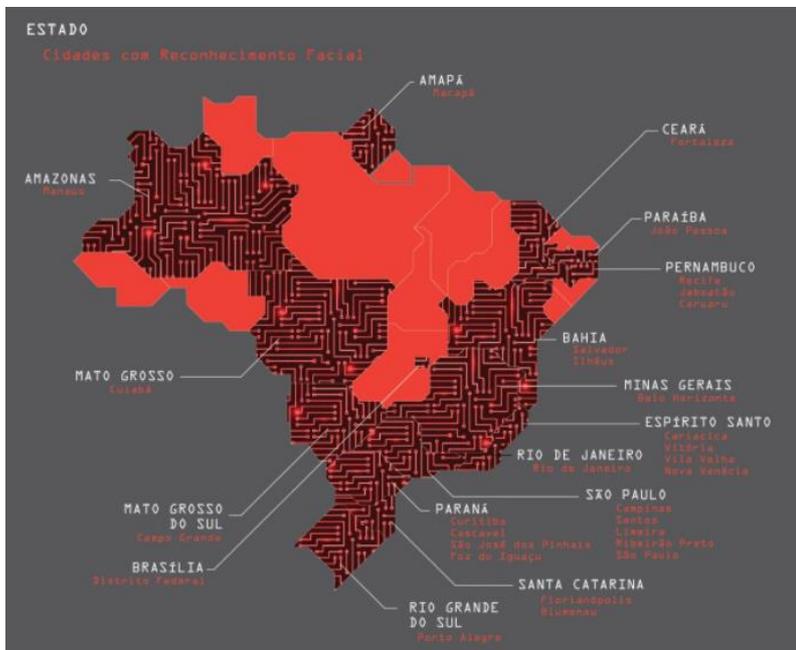
No Brasil, o RF vem sendo utilizado desde o ano de 2011, mas, tornou-se especialmente popular em 2019. As primeiras iniciativas de RF adotadas foram na área de transporte, em empresas intermunicipais que colocavam o reconhecimento como condição para o acesso aos serviços (HUREL, 2019). Nos últimos anos, o RF ganhou força fundamentalmente em aplicações na segurança pública, assim como para o acesso a locais e monitoramento por meio de câmeras. A partir desse cenário, e com a difusão dos conceitos de cidades inteligentes (CI) e cidades digitais, muitas cidades associaram os instrumentos de RF como alternativas para tornar factível a tutela da saúde e proteção dos cidadãos (RIZZON, 2017).

A adoção desses sistemas aumenta a capacidade de vigilância em setores urbanos e oportuniza um poder de polícia mais efetivo (MONTEIRO, 2021). Na Bahia, durante o carnaval um homem com mandado em aberto por tráfico de drogas foi capturado, alguns meses após flagra do Sistema de Reconhecimento Facial. A ferramenta tecnológica implementada em 2018, já ajudou na prisão de 210 pessoas com mandados por crimes violentos letais intencionais, crimes contra o patrimônio, crimes contra a criança e adolescentes, formação de quadrilha, além de venda ilícitos (SSP – BAHIA, 2021). Em 2020, durante o carnaval a cidade de São Paulo utilizou sistema de RF após inaugurar o Laboratório de Identificação Biométrica, Facial e Digital, no Instituto de Identificação Ricardo Gumbleton Daunt (IIRGD) (SÃO PAULO, 2020).

No mundo, diversas cidades já utilizam o RF nas áreas de segurança pública, transporte e controle de fronteiras (MONTEIRO, 2021). No Brasil, o RF tem sido utilizada tanto pela iniciativa privada quanto pela iniciativa pública. A partir do levantamento realizado em 2019, o Instituto Igarapé identificou os estados brasileiros que tem cidades utilizando o RF bem como

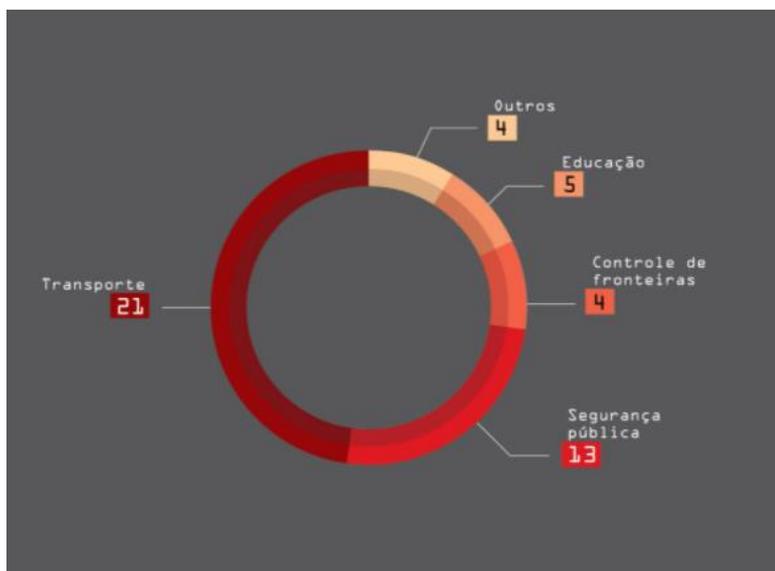
os quatro setores principais de uso do RF pelo setor público: educação, transporte, controle de fronteiras e segurança pública (Figura 1 e Figura 2).

Figura 1: Reconhecimento facial nas cidades brasileiras de 2011 a 2019



Fonte: Instituto Igarapé (2019).

Figura 2: Reconhecimento facial distribuído por setores



Fonte: Instituto Igarapé (2019).

Na distribuição, a maioria das cidades são as capitais dos estados. A região Sul e Sudeste são as que mais tem cidades utilizando a ferramenta. São Paulo e Paraná são os estados brasileiros com mais cidades utilizando o RF. São Paulo capital e Curitiba são cidades reconhecidas por terem iniciativas premiadas de cidades inteligentes (RANKING

CONNECTED SMART CITIES, 2020). A segurança pública e o transporte, seguidos de educação e controle de fronteiras são as áreas que atualmente utilizam o RF.

Em 2019 cerca de 70 equipamentos de RF foram instalados na região de fronteira entre o Brasil e o Paraguai. De acordo com a Receita Federal, a utilização de RF na cidade de Foz do Iguaçu, no oeste do Paraná, que faz fronteira com o Paraguai e a Argentina deve auxiliar o combate ao crime, identificando contrabando, tráfico de pessoas suspeitas e veículos que possuem alertas de furto ou roubo. Existe uma dinâmica de trocas e intercâmbios tanto culturais quanto econômicos, mas também sérias questões de ilegalidade e contrabando que fazem com que as fronteiras sejam estigmatizadas (MARTÍNEZ, 2020). Neste caso, é interessante que os governos busquem meios de modificar esse cenário. Positivamente, a aplicação de TICs já é uma prática no desenvolvimento de regiões de fronteira inteligentes (SOE, 2018). No caso da fronteira de Foz do Iguaçu, o sistema digitaliza os rostos das pessoas filmadas pelas câmeras e cruza as imagens com um banco de dados. Especificamente nesse projeto, que recebeu o nome de “Fronteira Tech”, o governo federal investiu cerca de R\$ 5 milhões utilizando tecnologia israelense que estava sendo testada no Parque Tecnológico de Itaipu (PTI). A iniciativa faz parte do Projeto Cidades Inteligentes, comandado pela Agência Brasileira de Desenvolvimento Industrial (ABDI) ligada ao Ministério da Economia (RPC, 2019).

Com uso de RF, em junho de 2021, teve início na ponte aérea Rio - São Paulo o projeto Embarque + Seguro 100% Digital. Esta é a primeira ponte aérea do mundo a usar a tecnologia de ponta a ponta. Nesse caso, o RF dispensa a apresentação do cartão de embarque e de documentos de identificação do passageiro e tem como objetivo tornar mais eficiente, ágil e seguro o processo de embarque nos aeroportos; na entrada da sala de embarque, ocorrerá de fato o procedimento de RF do passageiro para acesso à sala de embarque. Além desse projeto que é piloto nas cidades do Rio de Janeiro (RJ) e São Paulo (SP), a proposta de digitalização de embarque também foi testada em cidades como Florianópolis (SC), Salvador (BA) e Belo Horizonte (MG). O porta-voz da IDEMIA (empresa parceira de Biometria) aponta que a iniciativa do Governo Federal deve ser implementada em mais locais até o fim do ano, com o objetivo de melhorar a infraestrutura de aeroportos para privatização (TECMUNDO, 2019).

A empresa Hering, do ramo do vestuário, lançou a “Hering Experience”, uma loja conceito no Morumbi Shopping em São Paulo, onde utilizou a tecnologia de RF e detecção de calor para coletar e analisar os sentimentos dos clientes. Devido a essa ação, a empresa foi notificada pelo Instituto Brasileiro de Defesa do Consumidor (IDEC) para prestar esclarecimentos. Um dos questionamentos do órgão público é o de que a obtenção e análise dos dados deveria acontecer com o consentimento dos clientes. O IDEC toma como base a Lei Geral de Proteção de Dados Pessoais (LGPD) (FREITAS, 2019), entretanto no Brasil não existe legislação específica que regule o uso de RF (CAMARA DOS DEPUTADOS, 2020).

3 RECONHECIMENTO FACIAL E PRIVACIDADE

Como um reflexo do crescente aumento de aparatos de vigilância, a privacidade tende a diminuir e o tratamento massivo dos dados pessoais, tende a aumentar (MONTEIRO, 2021). Positivamente já existe uma preocupação por parte de alguns países de regular a privacidade de dados de seus cidadãos. No Brasil, a Lei Geral de Proteção aos Dados (LGPD) considera dado pessoal a informação relacionada a uma pessoa natural passível de identificação e dado pessoal sensível como o dado pessoal relacionado a origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, referente à saúde ou à vida sexual, genético ou biométrico (art. 5, I e II, LGPD). Com base na LGPD a única exceção para o fornecimento dos dados pessoais sem o consentimento do titular,

acontece quando se caracteriza como necessário para proteção da vida, da incolumidade física do titular ou de terceiros ou para garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos.

Outro aspecto tratado na LGPD e destacado por De Teffé (2020), é a finalidade da coleta dos dados, que deve ser de conhecimento prévio do cidadão, independente da base utilizada. O consentimento pelo cidadão determina como os dados pessoais podem ser tratados por terceiros, sendo um direito determinado na LGPD. No ano de 2019, o Projeto de Lei nº 865 previa a instalação obrigatória de câmeras de reconhecimento facial em todas as estações do Metrô da Cidade de São Paulo, bem como no interior dos vagões. O Projeto tinha como objetivo preservar a segurança das pessoas, evitando riscos à vida ou a integridade, e inibindo a ação de quadrilhas ou criminosos individuais, entretanto foi vetado pelo governador do Estado de São Paulo. As câmeras que já eram utilizadas também acabavam captando as reações dos cidadãos a propagandas e telas. No Brasil, a Central Única das Favelas (CUFA) descontinuou uma iniciativa de cadastramento biométrico e RF que visava cadastrar pessoas para receber doações após receber críticas através de redes sociais sobre a privacidade das pessoas e, situação de vulnerabilidade social.

Para Zeng *et al* (2019), embora o reconhecimento facial possa beneficiar a sociedade de muitas maneiras, a controvérsia e as preocupações estão aumentando, com destaque para:

- a) **Privacidade:** quando se trata de várias preocupações sobre reconhecimento facial, privacidade e segurança de dados são constantemente mencionadas;
- b) **Segurança:** embora considerado tipicamente como um meio de identificação de segurança, o reconhecimento facial não deve ser considerado suficientemente seguro;
- c) **Precisão:** ao considerar a aplicação de sistemas de reconhecimento facial em cenários do mundo real, os sistemas de reconhecimento facial podem não parecer ser tão confiáveis;
- d) **Viés:** além dos problemas de robustez e confiabilidade, o possível viés amplificado pela implantação de sistemas de reconhecimento facial traz consigo questões éticas;
- e) **Liberdade:** sistemas de vigilância alimentados por reconhecimento facial, se inadequadamente implantado ou sem todos os controles de segurança, não só falharão em salvaguardar eficazmente a segurança pública, mas também pode infringir a liberdade/privacidade das pessoas e fornecer uma fonte para abusos.

Surgem também os questionamentos: (i) se não existe uma lei específica para o uso do RF, a legislação sobre proteção de dados é eficiente quanto ao uso de dados pelos próprios governos? (ii) A população está mesmo ciente de quais dos seus dados são coletados? Sabe de que forma estes são coletados? (iii) E em caso de privatizações de empresas estatais como fica a manipulação dos dados de RF dos cidadãos que já foram coletados?

4 O CIDADÃO PANÓPTICO

O Panóptico, conceito proposto pelo filósofo Jeremy Bentham no final do século XVIII seria o desenho do cerceamento perfeito. O princípio desse conceito consiste em permitir que um simples observador (-opticum) possa veja todos (pan-) os detentos de uma instituição correcional, sem que eles saibam se foram vistos ou não. Embora seja fisicamente impossível para um único observador poder olhar para todos os detentos em suas celas ao mesmo tempo, o efeito é o de que os detentos não sabem quando podem estar sendo vigiados. Essa incerteza da vigilância causa forte impacto no comportamento dos indivíduos, pois eles se comportam

como se estivessem sendo observados e monitorados o tempo todo (OLIVO HERNÁNDEZ, 2014).

Diante da globalização e de ecossistemas cada vez mais digitais, o cidadão passa a agir como se estivesse em um panóptico, onde imagens e mensagens tornam sua identidade visível em grande escala, graças ao intercâmbio de informações pessoais, informações voluntárias e involuntárias relacionadas a sua imagem, gostos, e ideologias, entre outros interesses sociais diversos (CANO, 2018). Esse fenômeno pode ser vivenciado em cidades tidas como digitais ou que utilizam câmeras. Surge o questionamento: Até que ponto os cidadãos são conscientes do impacto do reconhecimento facial em suas vidas privadas?

Sob condições de vigilância, aqueles que detêm poder, administram e controlam os dados pessoais dos cidadãos e oferecem *insights* sem precedentes para suas vidas. Emerge então, uma nova dinâmica de poder; uma dinâmica baseada em uma ordem de "tem" e "não tem" entre aqueles que fornecem dados pessoais (cidadãos) e aqueles que os possuem e controlam (HINTZ; DENCİK; WAHL-JORGENSEN, 2017). Onde os dados podem ser coletados sem consentimento amparado pela legislação e comercializados ou utilizados para os mais diversos fins.

A sociedade de vigilância é um caso paradigmático de interação entre tecnologia e sociedade, onde os cidadãos passam a ser mais visíveis para os vigilantes, muitas vezes invisíveis, sendo submetidos a um controle constante e muitas vezes imperceptível (PRIOR, 2011). A vigilância também passa a ser um mecanismo utilizado pelo Estado, a fim de neutralizar ameaças e combater os níveis de insegurança, câmeras de vigilância e dispositivos de alta tecnologia passam a ser utilizados em locais públicos (CANO, 2018). Em sociedades que não contam com instituições sólidas ou que não tenham democracias representativas os reflexos negativos da vigilância podem ser ainda mais complexos.

O nexa Estado-cidadão exige um equilíbrio cuidadoso para que se possa proteger os direitos e liberdades cívicas e para que se possibilite a participação e a cidadania ativa. Entretanto, no contexto de *Big Data*, esse equilíbrio é ameaçado pois, a massiva coleta dos dados dos cidadãos também fortalece as agências estatais (HINTZ; DENCİK; WAHL-JORGENSEN, 2017) ou gigantes companhias de tecnologia. Fahey e Hino (2020) trazem o debate sobre priorizar a coleta autônoma de dados por parte das corporações de tecnologia e dos estados ou optar por dar poder de escolha aos cidadãos sobre a privacidade de seus dados. Também surge a preocupação com o domínio dos dados: quem deve ter a posse dos dados coletados? Empresas? Governos? Cidadãos? É seguro depender de grandes empresas de tecnologia para acessar dados em momentos de crise? Essa questão ficou ainda mais sensível com a pandemia de Covid-19 e a possibilidade de utilizar TICs para ações de controle da pandemia e de toque de recolher, por exemplo. Transformar as pessoas em números pode ser perigoso, uma vez que não será um número a indicar a posição de indivíduo na sociedade. Porém, argumenta-se que os indivíduos, uma vez transformados em dados, podem ser geridos e manipulados.

Os cidadãos também podem ter sua localização geográfica compartilhada bem como a autonomia na coordenação de suas atividades comprometidas pela dependência da interação do ser humano com as máquinas, que são cada vez mais autônomas (PRIOR, 2011). Um dos conceitos de CI assim como a dimensão cidadão inteligente, propõem que as pessoas que vivem nas cidades possam gozar de alto nível de qualificação; afinidade com a aprendizagem ao longo da vida; pluralidade social e étnica; flexibilidade; criatividade; participação na vida pública e coesão social (GIFFINGER *et al.*, 2007; CARAGLIU; DEL BO; NIJKAMP, 2011). Com a implementação de aparatos tecnológicos em iniciativas de CI ou com a criação (intencional ou não) de ambientes panópticos, a autonomia e a privacidade dos cidadãos, os direitos e garantias fundamentais são restringidos ou severamente comprometidos. Corre-se o risco de produzir

cidadãos panópticos. Essa realidade vai totalmente contra o que as CI se propõem a ser: cidades desenvolvidas, plurais e com elevada qualidade de vida para seus cidadãos.

5 RECONHECIMENTO FACIAL NO MUNDO: DESCONFIANÇA, PRECONCEITO RACIAL E DESCONTINUAÇÃO DE AÇÕES

Antes da pandemia de Covid-19 se transformar na principal pauta de debates atuais, as discussões sobre a tecnologia e sobre o RF estavam aquecidas. Na Europa, 80% das pessoas não gostam da ideia de compartilhar os dados de seus rostos com autoridades (NICOLÁS, 2020). Em 2021 a União Europeia considerou o RF como inteligência artificial de alto risco com potencial para ferir a democracia e que esta somente deve ser utilizada em casos extremos onde seja necessário procurar crianças desaparecidas, criminosos e pessoas em casos de ataques terroristas.

As autoridades da cidade de São Francisco nos Estados Unidos, proibiram o uso de RF depois de observar os danos que a tecnologia poderia causar às comunidades latinas ou afrodescendentes (FLYNN, 2020). Entre outros temas, o documentário intitulado *Coded Bias* disponível na plataforma de *streaming* Netflix problematiza a utilização do reconhecimento facial em cidades norte-americanas, inglesas e chinesas (CANALTECH, 2021). A questão do uso de RF em cidades, mais especificamente em comunidades periféricas e em pontos urbanos muitas vezes acontece sem a devida autorização e são relatadas ocorrências de identificações policiais equivocadas de pessoas negras como sendo criminosas. O documentário ainda levanta a questão de que existe um perigo eminente da tecnologia ser usada para reforçar ainda mais o racismo e a xenofobia onde o rosto das pessoas negras poderia ser associado ao de potenciais criminosos e a resistência dos cidadãos negros a ter seus dados coletados vista como suspeita. Também há indícios de que o RF não seja muito preciso com rostos negros e asiáticos. O fato do documentário retratar tais aspectos demonstra que este é um debate que está sendo feito por grupos e associações.

Em Boston, por exemplo, ocorreram os assassinatos de George Floyd, Breonna Taylor, Elijah McClain e de outras pessoas negras pela polícia geraram indignação nacional e internacional. A polícia repressiva dos Estados Unidos (assim como em muitos outros países) e a sociedade racista somados a possibilidade de uso de RF pela polícia poderiam trazer questões negativas, deste modo, Boston banuiu o RF. Essa decisão decorreu dos protestos e da moção de Boston para banir completamente a tecnologia devido às muitas possíveis consequências prejudiciais (FLYNN, 2020).

Mais recentemente, Portland, proibiu o reconhecimento facial em uma escala restrita, os cidadãos poderão receber até US\$ 1.000 se forem submetidos a uma varredura de reconhecimento facial da polícia que viole a nova proibição. Springfield é outra grande cidade que proibiu o uso de RF pela polícia e em fevereiro de 2020, a cidade colocou uma moratória à tecnologia com duração até 2025 (quando será reavaliada), impossibilitando o uso pela polícia. Essa mudança também ocorre em um momento de desconfiança para grandes empresas de tecnologia como a Amazon, que suspendeu o fornecimento de tecnologia de identificação facial à polícia durante o verão (FLYNN, 2020). O uso do RF por companhias aéreas também é problematizado nos Estados Unidos com o uso do "Biometric Air Exit" (BAE) devido à questão de ser usado para classificar cidadãos e "não-cidadãos" americanos e partida de cidadãos estrangeiros (TUCKER, 2020).

6 DESAFIOS E OPORTUNIDADES DO RECONHECIMENTO FACIAL

O emprego do RF vem suscitando algumas polêmicas, porém, algumas autoridades vêm apostando nesse tipo de tecnologia como instrumento sofisticado de controle em políticas públicas. Sobre essa questão, Ioannis Kouvakas da ONG Privacy International coloca: “a introdução do reconhecimento facial nas cidades é uma ideia radical e distópica que ameaça significativamente nossas liberdades e coloca questões fundamentais sobre o tipo de sociedade em que queremos viver”. A pesquisadora em democracia e tecnologia Thayane Guimarães, do Instituto de Tecnologia e Sociedade do Rio de Janeiro (ITS), alerta para a ausência de regulamentação. “O principal problema é a falta de uma legislação específica que garanta as liberdades individuais e a transparência no uso da tecnologia e proteção de dados pessoais” (MARASCIULO, 2020). A desconfiança sobre o que pode e o que não pode ser feito é grande entre a população, portanto a privacidade é um dos maiores desafios do uso dessa tecnologia em cidades.

Como visto, existem oportunidades do uso do RF em cidades. A tomada de decisão apoiada em dados já é amplamente debatida nas cidades inteligentes. O RF pode vir a fornecer dados para que as cidades possam tomar decisões. O uso das TICs também pode fazer com que a adoção de RF seja mais incentivada. Em busca no Web of Science com os filtros “Facial Recognition” e “Smart City” foi possível identificar 32 artigos, sendo a primeira publicação datada do ano de 2017. O RF é utilizado principalmente para as questões relativas à segurança (ZHANG *et al.* 2020) mas também pode ser aplicado na área da saúde (SUN; LI, 2020) e até mesmo para animais (NEETHIRAJAN; KEMP, 2021). O RF está relacionado à inteligência artificial, *machine learning* e à criação de algoritmos de reconhecimento, pode ser usado em locais como parques, ruas, praças, estádios, mas devido a vários casos de imprecisão são necessárias melhorias (LI *et al.* 2021). O uso de RF em cidades localizadas em regiões de fronteira é outra oportunidade.

A principal oportunidade do RF é a possibilidade de conferir mais resiliência às cidades. A resiliência é um dos aspectos relacionados às cidades inteligentes e até mesmo ao Objetivo de Desenvolvimento Sustentável (ODS) de número 11 que aponta a necessidade das cidades serem resilientes a desastres (provocados ou não pela ação humana) (ONU, 2015; SANTAELLA, 2016). Ações de combate às pandemias e localização de pessoas desaparecidas também podem se utilizar do RF. Apesar de que seja inegável que esta possa ser uma tecnologia útil, sem a devida regulação e cuidados, o RF pode violar a privacidade (DUARTE, 2019).

O fato é que existe uma linha tênue entre o reconhecimento facial “benigno” e os perigos relacionados à utilização desta tecnologia. O que preocupa é que negativamente ela pode ser até mesmo usada para a fragilização da democracia, reforçar preconceitos e estereótipos e para a perseguição política, por exemplo. Existe um grande desafio para as cidades neste sentido, o de tomar cuidado para não se tornarem potenciais *Big Brothers*. O direito à privacidade deve estar no topo das preocupações e cuidados de empresas e governos. Considera-se que as ações de RF também devam ser discutidas por especialistas, universidades e pela sociedade civil. À exemplo dos protestos contra o governo chinês ocorridos em Hong Kong no ano de 2019, ou do metrô de São Paulo, além de muito discutidas as ações de utilização do RF devem ser constantemente avaliadas. “A tecnologia traz benefícios, mas também muitos desafios de governança e comportamento” (CORTIZ, 2020). A partir de todo esse cenário, e se os exemplos de proibições anteriormente mencionadas continuarem, as cidades precisarão repensar o RF e se adaptar também visando a justiça social e racial (FLYNN, 2020). Questiona-se se as oportunidades podem superar os desafios do uso do RF, portanto, deve-se ter cautela com a utilização nas cidades.

7 CONSIDERAÇÕES FINAIS

Ao discorrer sobre o uso da ferramenta de RF em cidades foi possível abordar questões de privacidade, legislação, bem como oportunidades e ameaças para as cidades. As tecnologias de RF são ferramentas avançadas, mas estão relacionadas com questões legais e éticas e muitas vezes são utilizadas sem o consentimento e conhecimento das pessoas a que são submetidas. A facilidade com que esta pode ferir a privacidade e os direitos pessoais ainda é muito grande, sendo necessário tornar o processo mais transparente para os cidadãos. Mesmo que a América do Sul seja o continente cujos países mais utilizam o RF, por exemplo, a problematização sobre as questões de privacidade ainda estão muito mais centradas em países europeus e asiáticos.

No Brasil pouco se fala sobre o uso do RF. O uso do RF figura mais como ferramenta de apoio à segurança pública. Mesmo que a LGPD seja uma conquista para os cidadãos brasileiros é necessário que o debate sobre o uso do RF seja ampliado e que a aplicação de sanções em caso de descumprimento da lei seja eficiente. Considera-se que o debate do uso do RF em cidades não foi esgotado. Os atores e decisores dominantes continuam a controlar os desenvolvimentos urbanos “inteligentes”, enquanto os cidadãos muitas vezes não têm consciência e não têm conhecimento dos dados que são coletados. Os cidadãos como usuários das cidades devem ser parte integrante dos processos sócio tecnológicos que moldam o espaço urbano, participando da construção dos projetos em cidades inteligentes e sendo consultados sobre o uso do RF.

NOTAS DE FINAL DE TEXTO

Nota¹ Porque a CUFA interrompeu o uso de reconhecimento facial após polêmica. Fonte: <https://g1.globo.com/economia/tecnologia/noticia/2021/04/27/por-que-a-cufa-interrompeu-o-uso-de-reconhecimento-facial-apos-polemica.ghtml>

Nota² Reconhecimento facial deve ser banido, diz regulador de privacidade da EU. Fonte: <https://g1.globo.com/economia/tecnologia/noticia/2021/04/27/reconhecimento-facial-deve-ser-banido-diz-regulador-de-privacidade-da-ue.ghtml>

AGRADECIMENTOS

O presente trabalho foi realizado com o apoio da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior – Brasil (CAPES) – Código de financiamento 001.

REFERÊNCIAS

BUCKLEY, Ben; HUNTER, Matt. Say cheese! Privacy and facial recognition. **Computer Law & Security Review**, v. 27, n. 6, p. 637-640, 2011.

CÂMARA DOS DEPUTADOS. Jogo Rápido com Bibó Nunes – Segurança Pública. **Rádio Câmara**. Disponível em: <https://www.camara.leg.br/radio/programas/559577-bibo-nunes-psl-rs-seguranca-publica/?pagina=109> Acesso em: 20/06/2021.

CANALTECH. **Coded Bias usa didatismo para explicar terror por trás dos algoritmos. Por Felipe Demartini**. 2021. Disponível em: <https://canaltech.com.br/entretenimento/critica-coded-bias-netflix-182114/> Acesso em 21/06/2021.

CANO, Lucero Galvis. El Panóptico digital de la protección de datos personales en Colombia. **Revista Temas: Departamento de Humanidades Universidad Santo Tomás Bucaramanga**, n. 12, p. 125-140, 2018.

CARAGLIU, Andrea; DEL BO, Chiara; NIJKAMP, Peter. Smart cities in Europe. **Journal of Urban Technology**, v. 18, n. 2, p. 65–82, 2011. Disponível em: <https://doi.org/10.1080/10630732.2011.601117>

COSTA, Thalys Kialy da. O uso da tecnologia de reconhecimento facial e a violação a dados biométricos sob a luz da Lei Geral de Proteção de Dados. 2020.

CRIPPA, Margarete Esteves Nunes. Uso do reconhecimento facial aplicado à segurança pública no Brasil. **Controversias y Concurrencias Latinoamericanas**, v. 12, n. 22, p. 159-173, 2021.

DE TEFFÉ, Chiara Spadaccini; VIOLA, Mario. Tratamento de dados pessoais na LGPD: estudo sobre as bases legais. civilistica. com: **revista eletrônica de direito civil**, v. 9, n. 1, p. 1-38, 2020.

DUARTE, Júlia Tupynambá. A aplicação da tutela da proteção de dados pessoais no caso das portas interativas digitais do metrô de São Paulo. 2019.

FAHEY, Robert A.; HINO, Airo. COVID-19, digital privacy, and the social limits on data-focused public health responses. **International Journal of Information Management**. v. 55 2020.

FLYNN, Shanon. **13 Cities Where Police are banned from using facial recognition tech**. Innovation & Tech Today, Denver, CO, 2020. Disponível em: < <https://innotechtoday.com/13-cities-where-police-are-banned-from-using-facial-recognition-tech/> > Acesso em 12/06/2021.

FREITAS, Tainá. **Idec aciona Hering por uso de Reconhecimento Facial**. Startse.com, São Paulo, SP, 26/02/2019. Disponível em: < <https://www.startse.com/noticia/nova-economia/idec-aciona-hering-por-usar-tecnologia-de-reconhecimento-facial> > Acesso em: 14/06/2021

GIFFINGER, R. FERTNER, C; MILANOVIC, N; KALASEK, R; KRAMAR, H. Smart cities: ranking of European mid-sized cities **Smart cities Ranking of European medium-sized cities**. 2007. Disponível em: [https://doi.org/10.1016/S0264-2751\(98\)00050-X](https://doi.org/10.1016/S0264-2751(98)00050-X).

GOVERNO DA BAHIA. **Ferramenta auxilia na prisão de traficante**. Secretaria de Segurança Pública, Salvador, BA, 18/06/2021. Disponível em: < <http://www.ssp.ba.gov.br/2021/06/9845/Ferramenta-auxilia-na-prisao-de-trafficante.html> > Acesso em: 23/06/2021

HINTZ, Arne; DENCİK, Lina; WAHL-JORGENSEN, Karin. Digital citizenship and surveillance| digital citizenship and surveillance society—introduction. **International Journal of Communication**, v. 11, p. 9, 2017.

INSTITUTO IGARAPÉ. **Reconhecimento Facial no Brasil**. Instituto Igarapé, Rio de Janeiro, RJ, 01/03/2021. Disponível em: < <https://igarape.org.br/infografico-reconhecimento-facial-no-brasil/> > Acesso em: 17/06/2021

JANSSEN, M.; MATHEUS, R., ZUIDERWIJK, A. Big and Open Linked Data (BOLD) to Create Smart Cities and Citizens: Insights from Smart Energy and Mobility Cases. In.: Tambouris, E., Janssen, M., Scholl, H. J. et al. **Electronic Government**. Springer International Publishing. 9248: 79–90, 2015.

LI, Pan; ZHOU, Zhaojun; LIU, Qingji; SUN, Xiaoye; CHEN, Fuming; XUE, Wei. Machine Learning-Based Emotional Recognition in Surveillance Video Images in the Context of Smart City Safety. **Traitemet Du Signal**. V. 38. 2021.

MARASCIULO, Marília. **Reconhecimento facial: prós e contras da tecnologia que veio para ficar**. Revista Galileu, Rio de Janeiro, RJ, 22/06/2020. Disponível em: <<https://revistagalileu.globo.com/Tecnologia/noticia/2020/06/reconhecimento-facial-pros-e-contras-da-tecnologia-que-veio-para-ficar.html>> Acesso em: 12/06/2021

MARTÍNEZ, Mario Valero. Conflicto. In: **Palabras clave para el estudio de las fronteras Org. Benedetti, Alejandro Gabriel**. Ciudad Autónoma de Buenos Aires: Teseo Press, 2020.

MINISTÉRIO DA ECONOMIA. **Governo Federal, 2020**. Reconhecimento facial pelo aplicativo Meu gov.br é a primeira etapa da prova de vida dos aposentados. Disponível em: <<https://www.gov.br/economia/pt-br/assuntos/noticias/2020/agosto/reconhecimento-facial-pelo-aplicativo-meu-gov-br-e-a-primeira-etapa-da-prova-de-vida-dos-aposentados>>. Acesso em: 10/06/2021.

MONTEIRO, Guilherme Ornelas. Instrumentos de reconhecimento facial e os contornos da lei geral de proteção de dados ante a privacidade nas cidades (in) inteligentes. **Revista de Direito e Atualidades**, v. 1, n. 1, 2021.

NICOLÁS, Sanchez Elena. **Pandemic Speeds Calls for ban on facial recognition**. Eu Observer, Brussels, BE, 18/05/2020. Disponível em: <<https://euobserver.com/coronavirus/148387>> Acesso em: 14/06/2021

NEETHIRAJAN, Suresh; KEMP, Bas. Digital Twins in Livestock Farming. **Animals** v.11, 1008. 2021.

OLIVO HERNÁNDEZ, Oscar. **Del panóptico a la utopía de la smart city**. 2014.

PEREIRA, Gabriela Viale; CUNHA, Maria Alexandra; LAMPOLTSHAMMER, Thomas J.; PARYCEK, Peter; PRIOR, Hélder. Democracia deliberativa e vigilância eletrônica: da participação ao panóptico cibernético. **Communication Studies**, n. 10, 2011.

PURSHOUSE, Joe; CAMPBELL, Liz. Privacy, crime control and police use of automated facial recognition technology. **Criminal Law Review**, v. 2019, n. 3, p. 188-204, 2019.

RANKING CONNECTED SMART CITIES. Disponível em: <https://ranking.connectedsmartcities.com.br/resultados.php> Acesso em: 20/06/2021, 2020.

RIVERO-ANGELES, Mario E. et al. Mobile Clustering Scheme for Pedestrian Contact Tracing: The COVID-19 Case Study. **Entropy**, v. 23, n. 3, p. 326, 2021.

RIZZON, F., BERTELLI, J., MATTE, J., GRAEBIN, R. E., & MACKE, J. (2017). Smart City: um conceito em construção. **Revista Metropolitana de Sustentabilidade (ISSN 2318-3233)**, 7(3), 123-142.

RPC Foz do Iguaçu. Câmeras com Tecnologias de reconhecimento facial e identificação de placas começam a funcionar na ponte da Amizade. **Rede Paranaense de Televisão, Foz do Iguaçu, 2019**. Disponível em: <https://g1.globo.com/pr/oeste-sudoeste/noticia/2019/12/14/cameras-com-tecnologias-de-reconhecimento-facial-e-identificacao-de-placas-comecam-a-funcionar-na-ponte-da-amizade.ghtml> Acesso em: 12/06/2021

SÃO PAULO. Governo de SP inaugura Laboratório de Identificação Biométrica – Facial e Digital. **Site oficial da prefeitura municipal de São Paulo**. 2020. Disponível em: <https://www.saopaulo.sp.gov.br/sala-de-imprensa/release/governo-de-sp-inaugura-laboratorio-de-identificacao-biometrica-facial-e-digital/> Acesso em: 21/06/2021

SERPRO. Seu consentimento é Lei, 2021. Disponível em: <<https://www.serpro.gov.br/lgpd/cidadao/quais-sao-os-seus-direitos-lgpd>>. Acesso em: 16/06/2021.

SOE, Ralf Martin. Smart cities: From silos to cross-border approach. **International Journal of E-Planning Research**, v. 7, n. 2, p. 70–88, 2018. Disponível em: <https://doi.org/10.4018/IJEPR.2018040105>

SUN, Mingsi; LI; Dongmei. Smart face identification via improved LBP and HOG features. **Internet Technology Letters**. v.4 Maio de 2021.

TECMUNDO. Brasil é pioneiro no uso de reconhecimento facial em aeroportos. **Tech Mundo, São Paulo, SP, 2021**. Disponível em: <https://www.tecmundo.com.br/mobilidade-urbana-smart-cities/219316-brasil-usa-reconhecimento-facial-ter-aeroportos-embarque-digital.htm>. Acesso em 21/06/2021

TESTA, Maurício Gregianin. Increasing collaboration and participation in smart city governance: a cross-case analysis of smart city initiatives. **Information Technology for Development**, v. 23, n. 3, p. 526–553, 2017.

TUCKER, Aron. The Citizen Question: Making Identities Visible Via Facial Recognition Software at the Border. **IEEE Technology and Society Magazine**. v. 39. p.52-59. 2020.

UNITED NATIONS. “**GOAL 11: Sustainable Cities and Communities | UN Environment.**” 2015.

ZENG, Jiwei; YAN, Xiaodan; CHENG, Zelei; SHEN, Xueqi. A face recognition algorithm based on feature fusion. **Concurrency and Computation-Practice & Experience**. 2020.