Revista da Faculdade de Direito do Sul de Minas

TECNOLOGIA DE RECONHECIMENTO FACIAL COMO POLÍTICA DE SEGURANÇA PÚBLICA: O CASO DO METRÔ DE SÃO PAULO

FACIAL RECOGNITION TECHNOLOGY AS A PUBLIC SECURITY POLICY: THE CASE OF THE SÃO PAULO SUBWAY

*Denis Cortiz da Silva**
*Gianfranco Faggin Mastro Andréa***
*Wagner Wilson Deiró Gundim****

RESUMO

O presente artigo tem como escopo o estudo da aplicação da tecnologia do reconhecimento facial como política de segurança pública no âmbito do metrô do Estado de São Paulo. O problema de pesquisa consiste na indagação: é possível a utilização do reconhecimento facial pelo metrô do Estado de São Paulo? O objetivo do estudo consiste em verificar a legalidade e/ou constitucionalidade da concessão do serviço de monitoramento por meio de reconhecimento facial. As metodologias utilizadas foram a de revisão bibliográfica e estudo de caso. Concluiu-se que em função do Metrô de São Paulo não fazer parte do sistema de segurança pública estadual, apresenta-se ilegal e inconstitucional a concessão para o monitoramento via tecnologia de reconhecimento facial dos cidadãos consumidores do serviço de transporte público, oportunidade em que se oferece possível solução para a questão.

Palavras-chave: direito à privacidade; direito à proteção de dados pessoais; reconhecimento facial; segurança pública.

ABSTRACT

This article aims to study the application of facial recognition technology as a public safety policy in the context of the São Paulo State subway. The research problem consists in the question: is it possible to use facial recognition by the subway of the State of São Paulo? The aim of this study is to verify the legality and/or constitutionality of the granting of the monitoring service through facial recognition. The methodologies used were bibliographic review and case study. It was concluded that because the São Paulo subway is not part of the state public security system, it is illegal and unconstitutional to grant for monitoring via facial cognition technology of citizens who are consumers of the public

* Graduação em Direito pela Universidade Presbiteriana Mackenzie, Mestre em Direito Político e Econômico pela Universidade Presbiteriana Mackenzie. Professor de Direito da Universidade Paulista e Universidade São Judas. Delegado de Polícia. Lattes: http://lattes.cnpq.br/0154088457124074. ORCID: 0000-0002-3638-5681. E-mail: dcortiz1981@gmail.com.

** Graduação em Direito pela Universidade Presbiteriana Mackenzie, Especialização em Direito Público pela Faculdade de Direito Damásio de Jesus, Mestre e Doutorando em Direito Político e Econômico pela Universidade Presbiteriana Mackenzie. Professor de Direito da Universidade Paulista. Analista do Ministério Público da União. Lattes: http://lattes.cnpq.br/9702790239703189. ORCID: 0000-0003-4817-0298. E-mail: professorgianfaggin@gmail.com.

*** Graduação em Direito pela Universidade Anhembi Morumbi, Mestre em Direito Político e Econômico pela Universidade Presbiteriana Mackenzie, tendo sido bolsista CAPES. Doutor em Filosofia do Direito pela Pontifícia Universidade Católica de São Paulo (PUC/SP). Doutorando em Direito Constitucional pela Faculdade de Direito da Universidade de São Paulo (FADUSP). Professor de Direito Constitucional, Ciência Política e Fundamentos do Direito Eleitoral na Universidade Anhembi Morumbi. Sócio Fundador do Gundim & Ganzella Sociedade de Advogados. Lattes: http://lattes.cnpq.br/9744255875865234. ORCID: 0000-0003-4309-2788. E-mail: wagner.gundim@adv.oabsp.org.br.

transportation service, an opportunity in which a possible solution to the issue is offered.

Key-words: right to privacy; right to protection of personal data; facial recognition; public security.

INTRODUÇÃO

O desenvolvimento tecnológico vem crescendo a uma velocidade nunca vista antes. São instrumentos tecnológicos que vêm sendo colocados à disposição da sociedade alterando nossa dinâmica de vida de forma profunda. Alguns denominam este novo momento da humanidade como Quarta Revolução Industrial.

A Inteligência Artificial – IA que há algumas décadas parecia objeto apenas de filmes de ficção científica, apresentam-se atualmente muito presente no nosso dia a dia. Um dos desdobramentos da Inteligência Artificial é a tecnologia do reconhecimento facial.

O reconhecimento facial é instrumento tecnológico capaz de inúmeras utilizações, porém vêm sendo aplicado por meio de monitoramento de vídeo em locais públicos para fins de garantia da segurança pública. Valendo-se de um prévio banco de dados de imagens é possível que a IA do reconhecimento facial relacione e identifique indivíduos constantes de aludidos acervos. Tal recurso vem sendo utilizado para o cumprimento de mandados de prisão, por exemplo.

É sabido que a questão da vigilância e privacidade não são temas novos ou recentes e que vêm sendo discutidos há décadas. Ocorre que no momento de inflexão tecnológica hodierno, afigura-se medida de rigor a reflexão e rediscussão acerca de conceitos que tomam novos contornos com a aplicação tecnológica, notadamente em se tratando de direito à privacidade, intimidade, bem como direito à imagem e o direito a proteção de dados pessoais.

Diante deste cenário, o presente estudo busca analisar o caso da implementação do reconhecimento facial no metrô do Estado de São Paulo. O problema de pesquisa consiste em verificar a (i) legalidade e/ou (in) constitucionalidade na atribuição ao Metrô de São Paulo de atividades próprias da Segurança Pública. Para tanto, utilizamos as metodologias de revisão bibliográfica e de estudo de caso.

Na primeira parte do estudo contextualiza o momento de inflexão quanto às tecnologias e avanços tecnológicos disruptivos que aqui se convencia denominar de Quarta Revolução Industrial, bem como aborda o conceito e funcionamento do reconhecimento facial.

Na segunda parte, apresenta o debate que vigora na academia acerca da questão dos limites da vigilância na Sociedade da Informação e conceitos de privacidade e proteção de dados pessoais. Por fim, discorre acerca da aplicação da tecnologia do reconhecimento facial no metrô de São Paulo, oportunidade em que investiga a legitimidade em sua implantação e possível legalidade e/ou constitucionalidade à luz das atribuições próprias dos órgãos de Segurança Pública.

Novas tecnologias e a quarta revolução industrial: reconhecimento facial

A humanidade vive em uma quadra da história em que existem inúmeras incertezas. Por um lado, os recursos naturais e questões ambientais parecem advertir para um obscuro futuro. Ao mesmo tempo, o surgimento de novas tecnologias - em cada vez menos tempo - aponta para a possibilidade de desenvolvimento sustentável, automatização de trabalhos repetitivos e superação de diversos problemas relacionados, desde saneamento básico, passando pela saúde, segurança pública até a educação.

A capacidade das novas tecnologias, portanto, inauguram um novo período para a humanidade. Dentre as novidades é possível apontar para: Inteligência Artificial (IA), robótica, a internet das coisas (IoT, do inglês), aprendizado de máquina (*machine learning*), veículos autônomos, impressão 3D, nanotecnologia, biotecnologia, ciência dos materiais, armazenamento de energia, computação quântica e tecnologias de *big data* (grande volume de dados estruturados ou não)[1].

Trata-se de profundas mudanças que estão no seu início, mas são inevitáveis. A questão é que na história nunca houve um período tão promissor e ao mesmo tempo tão perigoso. O momento é de ruptura e inovação que moldarão o futuro. No contexto histórico o termo "revolução" significa mudança abrupta e radical e historicamente as revoluções têm ocorrido diante de inovações tecnológicas e novas formas de perceber o mundo que culminam em alterações estruturais tanto na sociedade, quanto no sistema econômico[2].

A primeira revolução foi a agrícola, oportunidade em que houve a transição da busca por alimentos para a agricultura há cerca de dez mil anos, por meio da domesticação dos animais. Tal ruptura possibilitou a urbanização e ao surgimento de cidades. Tal revolução foi seguida por uma série de revoluções industriais. O ponto em comum entre elas foi a transição da força muscular para a energia mecânica[3].

A primeira revolução industrial deu-se entre 1760 e 1840. Principal fator de ruptura com o paradigma até então existente foi a construção das ferrovias e invenção da máquina à vapor, o que proporcionou a produção mecânica. A segunda revolução industrial teve início no final do século XIX e início do século XX. O momento de inflexão deu-se com o advento da eletricidade e a linha de montagem, o que garantiu a produção em massa. Já a terceira revolução industrial, ocorreu a partir da década de 1960 e é denominada de revolução digital, pois as mudanças decorreram do desenvolvimento da computação em *mainframe* (meados da década de 1960), computação pessoal (década de 1970 e 1980) e da internet na década de 1990[4].

Para Klaus Schwab vivemos na atualidade uma quarta revolução industrial com início na virada do século e baseada na revolução digital. Tem como principal caraterísticas uma internet espraiada e móvel; inteligência artificial e aprendizagem

[1]GAMBA, João Roberto Gorini**.** *Democracia e tecnologia*: impactos da quarta revolução industrial. Rio de Janeiro: Lumen Juris, 2020, p. 76.
[2]SCHWAB, Klaus. *A quarta revolução industrial*. Tradução Daniel Moreira Miranda. São Paulo: Edipro, 2016, p. 15.
[3] Idem.
[4]GAMBA, João Roberto Gorini**.** *Op cit.*, p. 70-75.

automatizada. De fato, segundo o autor, as tecnologias digitais evoluíram de tal modo que provocaram uma radical ruptura com o que se tinha conhecimento acerca de computadores com a terceira revolução industrial. Isto porque as tecnologias digitais estão mais sofisticadas e integradas, causando profundas mudanças sociais e econômicas[5].

Vivemos num ponto de inflexão com as novas tecnologias digitais e a quarta revolução industrial diferencia-se das anteriores pois o que testemunhamos "é a fusão dessas tecnologias e a interação entre os domínios físicos, digitais e biológicos".[6] Klaus Schwab também aponta três razões que sustentam a ocorrência de uma quarta revolução industrial:

> **- Velocidade:** ao contrário das revoluções industriais anteriores, esta evolui em um ritmo exponencial e não linear. Esse é o resultado do mundo multifacetado e profundamente interconectado em que vivemos; além disso, as novas tecnologias geram outras mais novas e cada vez mais qualificadas.
> **- Amplitude e profundidade:** ela tem a revolução digital como base e combina várias tecnologias, levando a mudanças de paradigma sem precedentes da economia, dos negócios, da sociedade e dos indivíduos. A revolução não está modificando apenas o 'o que' e o 'como' fazemos as coisas, mas também 'quem' somos.
> **- Impacto sistêmico:** ela envolve a transformação de sistemas inteiros entre países e dentro deles, em empresas, indústrias e em toda a sociedade.

João Roberto Gorini Gamba destaca que a centralidade da quarta revolução industrial pode ser encontrada na capacidade de gerar e processar as informações de dados, ou seja, mudamos da noção de Sociedade da Informação que se pautava pela importância econômica, política e social da informação para instalarmos a novel Sociedade de Dados (*Data Society*), por meio da qual assume a dianteira "a relevância social da geração, captação, propagação e, principalmente, da análise de dados"[7].

Dentro de todas essas mudanças estruturais é sabido que a tecnologia da Inteligência Artificial cresce a uma taxa de 60 % ao ano.[8] Por sua vez, a tecnologia do reconhecimento facial é uma das aplicações da tecnologia de Inteligência Artificial (IA)[9]. A IA é tecnologia que se vale da biometria[10] e conforme destacam Cleiton Correia Viana, Valdir Silva Conceição e Ângela Machado Rocha:

[5]SCHWAB, Klaus. *Op cit*., p. 16.
[6] Idem.
[7] GAMBA, João Roberto Gorini**.** *Op cit*., p. 78-79.
[8] VIANA, Cleiton Correia; CONCEIÇÃO, Valdir Silva; ROCHA, Ângela Machado. Reconhecimento Facial e a Relativização do Direito da Imagem**.** *REVISTA INGI***.** Vol.3, n.3, p.436-450. Jul/Ago/Set, 2019, p. 437. Disponível em: http://ingi.api.org.br/index.php/INGI/article/view/50. Acesso em: 11 jul. 2020.
[9] "A IA é um ramo recente da ciência e da engenharia originária da década de 1950 e que tem o objetivo de analisar e de interpretar os dados complexos, simular ou reproduzir a inteligência humana em máquina e traz como resultados o diagnóstico, o tratamento e a previsão de resultados" (CONCEIÇÃO, *Valdir Silva; NUNES, Edna Maria; ROCHA, Angela Machado.* O Reconhecimento Facial como uma das Vertentes da Inteligência Artificial (IA): um estudo de prospecção tecnológica. *Cadernos de Prospecção***.** Salvador, v. 13, n. 3, p. 745-758, junho, 2020. p. 746).
[10] "A biometria é um tipo de medição que utiliza as medidas de determinada parte do corpo e faz a comparação de dois conjuntos de dados, utilizando-se dos dados armazenados em um banco de dados de imagem. Tratando da descrição do produto, existem algumas maneiras de identificação utilizando a biometria, assim pode-se constatar o uso das digitais para desbloquear acesso ao conteúdo de smartphones, oportunizando a realização até mesmo de operações bancárias, emprego no sistema de votação, dentre

> É um sistema inventado por Woodrow Wilson Bredsoe em 1964, em conjunto com Helen Chan Wolf e Charles Bisson, cujo objetivo é identificar as pessoas através de imagem ou vídeo e tem sido estudada e pesquisado de forma ativa a partir da década de 1970, inicialmente com uma abordagem baseada em características, definido por uma representação baseada em proporções da distância, área e ângulo. O segundo tipo de pesquisa é baseado em holísticas decorrentes de estatísticas e IA que aprendem e executam um conjunto de dados de imagens do rosto. As técnicas atualmente mais utilizadas são as redes neurais. O rosto é comparado com base na geometria facial, incluindo as distâncias e proporções entre os olhos e da sobrancelha, comprimento da linha da mandíbula, tamanho do crânio, linha do cabelo, largura do nariz, da boca, do lábio entre outras 80 bases faciais ou pontos nodais, a tecnologia compara a imagem real capturada, com as inúmeras imagens pesquisadas e que já estão inseridas no programa de reconhecimento. Ela possui o poder de identificar faces, mesmo que estejam disfarçadas com óculos, peruca, boné, chapéu e lenço[11].

Portanto, o sistema de reconhecimento facial necessita de uma base de dados prévia para que realize a leitura dos pontos faciais de uma pessoa, oportunidade em que o codifica em uma sequência digital capaz de gerar um número de identificação individualizado. Todos os momentos em que aquele indivíduo surgir em uma câmera as suas informações faciais serão comparadas com as existentes no banco de dados viabilizando sua identificação com alto grau de eficácia.

Fato é que a tecnologia encimada vem sendo utilizada por Estados para monitorar a circulação de pessoas em ambientes públicos, a fim de localizar, identificar e permitir a abordagem de indivíduos que ostentem mandados de prisão em aberto para cumprimento da pena, por exemplo.

Neste passo, alguns países e, agora no Brasil alguns Estados-membros,[12] já vêm se utilizando da tecnologia do reconhecimento facial como instrumento facilitador para garantia da execução da pena, evitando prescrição intercorrente ou ainda prescrição da pretensão executória, buscando com isso diminuir a sensação de impunidade.

No passado o policial humano apenas dependia de suas capacidades cognitivas e buscava prevenir, investigar e solucionar crimes. Era necessário maior treinamento e fatores intrinsecamente humanos para um bom desempenho profissional. Com a tecnologia disruptiva que acompanha a quarta revolução industrial, as novas ferramentas tecnológicas proporcionam uma verdadeira *cyborgização* do cotidiano. A tecnologia do reconhecimento facial permite "se descobrir no meio da multidão as pessoas, dado que a

outras inúmeras aplicações. Pode-se também utilizar o *scanner* da íris e retina para fazer a identificação para acessar determinados ambientes, pois essas partes dos olhos permanecem quase inalteradas durante toda a vida, o que o coloca como uma das partes mais confiáveis para a autenticação biométrica. Como derivação dessa biometria existe o reconhecimento facial com a codificação da face por um software. As duas primeiras técnicas dependem da cooperação ou conhecimento do indivíduo, enquanto que o reconhecimento facial não precisa dessas duas condições" (VIANA, Cleiton Correia; CONCEIÇÃO, Valdir Silva; ROCHA, Ângela Machado. O*p cit.*, p. 438).

[11] VIANA, Cleiton Correia; CONCEIÇÃO, Valdir Silva; ROCHA, Ângela Machado. *Op cit.*, p. 443.

[12] Tal tecnologia foi utilizada durante o Carnaval da Bahia em 2019 pela Secretaria de Segurança Pública do Estado (BRASIL. Câmeras de reconhecimento facial vão ajudar a identificar criminosos no carnaval. *Correio da Bahia*, Salvador, 26 fev. 2019. Disponível em: https://www.correio24horas.com.br/noticia/nid/cameras-de-reconhecimento-facial-vao-ajudar-a-identificar-criminosos-no-carnaval/. Acesso em 10 jul. 2020).

transparência neste local é ampliada, chegando ao ponto de retirar o que antes se conhecia como esfera privada do sujeito [...]"[13].

Os sistemas que se valem de algoritmos[14] como o do reconhecimento facial decorrente da IA não são imunes a erros e este fator gera certa repulsa a sua utilização.[15] Diversos casos foram relatados em que o reconhecimento facial "enganou-se" proporcionando o encarceramento equivocado. Isto ocorreu porque os algoritmos podem reproduzir preconceitos de raça (pessoas negras) e gênero (mulheres)[16]. E não só isso, João Roberto Gorini Gamba alerta:

> [...] até mesmo os critérios de classificação e identificação de dados podem ser embebidos de preconceito do programador e, com isso, determinar o viés da análise e dos resultados obtidos, sobre os quais se estruturará a decisão.
> Nesse assunto, é importante destacar que a alimentação dos dados é feita com base em dados do passado visando conduzir ações futuras. Nesse caso, é comum verificar que as tecnologias de big data acabam por perpetuar a desigualdade ou o fator gerador daquelas conclusões tiradas, na medida em que criam um círculo vicioso em torno de suas causas[17].

De qualquer forma, trata-se, portanto, da utilização da tecnologia do reconhecimento facial como política pública para captura de indivíduos e garantia do cumprimento das penas impostas.

Diante disso, aborda-se a seguir a discussão sobre a questão da coleta de dados pessoais – incluídos aqui os dados de imagem facial – e a possível violação de direitos a privacidade e proteção de dados pessoais.

[13] MORAIS DA ROSA, Alexandre. A questão digital: o impacto da inteligência artificial no Direito. *Revista de Direito da Faculdade Guanambi*, Guanambi, v. 6, n. 02, e259, jul./dez. 2019, p. 12. DOI: https://doi.org/10.29293/rdfg.v6i02.259. Disponível em: http://revistas.faculdadeguanambi.edu.br/index.php/Revistadedireito/article/view/259. Acesso em: 12 jul. 2020.

[14] Como explicam Bruna Dias Franqueira, Ivar A. Hartmann e Lorena Abbas da Silva: "De modo geral, para que alguém possa ser identificado via reconhecimento facial, primeiro um algoritmo deve localizar o rosto da pessoa na imagem –processo chamado de detecção de face. Uma vez detectada, essa face é "padronizada" –dimensionada e alinhada –para que todas as outras faces processadas pelo algoritmo estejam na mesma posição, facilitando a comparação dos rostos. Em seguida, o algoritmo extrai as características da face que podem ser quantificadas de forma numérica, como a distância entre os olhos, nariz e boca ou a textura da pele. A padronização é importante pois tais características serão analisadas em suas variações estatísticas (KLARE et al., 2012, p. 1791)3, uma vez que os elementos tenham sido transformados em representações matemáticas, conectados de forma individualizada. Por último, o algoritmo examina grupos de imagens de rostos e emite uma pontuação que reflete a semelhança entre as características das faces que constam no banco de dados (DAUGHERTY *et al*., 2016, p. 9) e aquela que está sendo submetida a identificação" (ABBAS DA SILVA, L.; FRANQUEIRA, B. D.; HARTMANN, I. A. O que os olhos não veem, as câmeras monitoram: reconhecimento facial para segurança pública e regulação na América Latina. Revista *Digital de Direito Administrativo*. [S. l.], v. 8, n. 1, p. 171-204, 2021. DOI: 10.11606/issn.2319-0558.v8i1p171-204. Disponível em: https://www.revistas.usp.br/rdda/article/view/173903. Acesso em: 14 fev. 2022).

[15] GAMBA, João Roberto Gorini**.** *Op cit*., p. 82.

[16] THOMPSON, Isobel. The future of your face. *Life*, 25 jun. 2019. Disponível em: https://theface.com/life/the-future-of-your-face. Acesso em: 12 jul. 2020.

[17] GAMBA, João Roberto Gorini**.** *Op cit*., p. 82.

Direito à proteção de dados e direito à privacidade: velhos problemas, novas abordagens

A evolução tecnológica tornou possível, por meio do *Big Data* (organização de dados de maneira mais escalável), a construção de uma economia da vigilância que transforma o cidadão como um simples observador de suas próprias informações[18]. Com isso, os dados pessoais dos cidadãos passaram a representar verdadeiros ativos para as grandes corporações, de modo que a posse de quantidades elevadas de dados é sinônimo de poder.

De fato, o amplo acesso aos dados pessoais torna possível o aprimoramento do próprio negócio, uma vez que além de se valerem de tais informações para identificar o perfil, características e rotina de consumo de seu público-alvo, as empresas também podem negociar tais dados com outras corporações[19]. Ademais, o usuário da internet está a todo momento sendo monitorado, seja pelas "marcas digitais" deixadas onde navega, o que permite um direcionamento personalizado de publicidade de bens e serviços, seja pela utilização das redes sociais, as quais em função de suas próprias políticas de geolocalização e conservação de dados (geralmente pelo termo ativar rastreamento) acabam facilitando um monitoramento constante do perfil de consumo (não apenas de produtos e serviços, mas também de informações), e até mesmo de lugares por eles frequentados. É nesta camada nebulosa que a maioria dos problemas relativos à privacidade e proteção de dados se constitui.

Em função disso, de modo a atenuar essa possível tensão entre o direito à privacidade de dados pessoais e a necessidade de aprimoramento das ferramentas tecnológicas, foi possível constatar a tentativa de, pelo direito, regulamentar/normatizar a temática, o que é exemplificado tanto pelo Regulamento Geral de Proteção de Dados Europeu (RGPD) – modelo utilizado por outros países como base de suas legislações nacionais -, como pela Lei Geral de Proteção de Dados no Brasil, que também tem como base o RGPD. Tal é a relevância da proteção de dados na atualidade que recentemente os dados pessoais foram alçados a categoria de direito fundamental constitucional no Brasil, conforme consta da emenda constitucional nº 115/2022[20].

Com isso, a preocupação central de tais normativações está relacionada a uma possível má utilização dos dados pessoais[21], pelo governo ou outras entidades, sem o

[18] BIONI, Bruno Ricardo. *Proteção de dados pessoais:* a função e os limites do consentimento. 2. ed. Rio de Janeiro: Forense, 2020. p. 12.

[19] Sobre o uso do reconhecimento facial para além dos discursos de segurança interna, isto é, compreendendo também a sua utilização para fins comerciais, ver: BECK, Cesar Augusto Moacyr Rutowitsch; BOFF, Murilo Manzoni; PIAIA, Thami Covatti. Os (ab)usos da tecnologia de reconhecimento facial na segurança pública e na prestação de serviços a partir da pandemia de COVID-19. *Revista Pensamento Jurídico.* São Paulo, v. 15, n. 2, mai./ago. 2021.

[20] BRASIL. Emenda Constitucional nº 115, de 10 de fevereiro de 2022. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/Emendas/Emc/emc115.htm. Acesso em 14 fev. 2022.

[21] Rosane Leal da Silva e Fernanda dos Santos Rodrigues da Silva, por exemplo, apontam para os desdobramentos do uso da tecnologia de reconhecimento facial em um sistema penal seletivo e racista (CF. SILVA, Rosane Leal da; SILVA, Fernanda dos Santos Rodrigues da. Reconhecimento facial e segurança pública: os perigos do uso da tecnologia no sistema penal seletivo brasileiro. *Anais do 5º Congresso*

consentimento dos usuários, tornando-o verdadeiro cidadão/homem de vidro (transparente e sem qualquer segredo a ser preservado)[22].

Aqui é preciso acentuar que essa economia da vigilância é desenvolvida no contexto de uma Sociedade da Vigilância, a qual, por sua vez, pressupõe um controle social contínuo por meio de novas tecnologias tais como Big Data, 5G, drones, reconhecimento facial, entre outras[23].

De fato, o principal objetivo dessa sociedade da vigilância é a classificação[24]. Para Bauman a contemporaneidade dentro do contexto de modernidade líquida apresenta o conceito de vigilância líquida, ou seja, para o autor vive-se num momento em que tudo que é sólido se desmancha no ar, e, consequentemente, todas as formas sociais se desmancham mais depressa que a velocidade com que se criam novas formas.

Saindo, portanto, do conceito de vigilância sólida do panóptico idealizado por Jeremy Bentham e, posteriormente aperfeiçoado por Michel Foucault, parte-se – a partir de Gilles Deleuze - para a concepção de sociedade de controle que cresce não como uma árvore, mas sim como ervas daninhas.[25] A partir daqui a vigilância líquida pode ser compreendida, uma vez que o "inspetor" não se encontra fixo por trás do panóptico, mas agora pode escapulir por domínios inalcançáveis. É por isso que segundo Bauman estamos diante da era do pós-pan-ótico[26].

As novas tecnologias, assim, dão uma falsa impressão de liberdade, aprisionando os cidadãos de uma maneira muito mais efetiva, por meio da constante vigilância, mas uma vigilância dinâmica e que se amolda constantemente. Diferente da vigilância sólida que consolida o poder de vigilância em uma figura sólida como o Grande Irmão de Orwell[27], a vigilância líquida dilui-se pela multiplicação de pequenos irmãos, diante de

Internacional de Direito e Contemporaneidade: mídias e direitos da sociedade em rede. UFMS – Universidade Federal de Santa Maria, 2019).

[22] RODOTÁ, Stefano. *A vida na sociedade da vigilância* – a privacidade hoje. Organização, seleção e apresentação de Maria Celina Bodin de Moraes. Tradução: Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008. p. 47.

[23] Nesse sentido, Stefano Rodotá destaca que: "A novidade é radical. Os riscos da sociedade da vigilância ligam-se tradicionalmente ao uso político de informações para controlar os cidadãos, o que qualifica tais sociedades como autoritárias e ditatoriais. Na perspectiva que vai se delineando, ao contrário, a ideia de vigilância invade cada momento da vida e se apresenta com um traço próprio das relações de mercado, cuja fluidez diz respeito à possibilidade de dispor livremente de um conjunto crescente de informações. Materializa-se assim a imagem do 'homem de vidro', o verdadeiro cidadão desse novo mundo. Uma imagem que, não por acaso, provém diretamente do tempo do nazismo e que propõe uma forma de organização social profundamente alterada, uma espécie de transformação irrefreável da 'sociedade da informação' em 'sociedade da vigilância'" (RODOTÁ, Stefano. *Op cit*., p. 113).

[24] *Ibidem*, p. 114.

[25] BAUMAN, Zygmunt. *Vigilância Líquida***:** diálogos com David Lyon. Tradução: Carlos Alberto Medeiros. Rio de Janeiro: Zahar, 2014. p. 7.

[26] "O pan-óptico é apenas um modelo de vigilância. A arquitetura das tecnologias eletrônicas pelas quais o poder se afirma nas mutáveis e móveis organizações atuais torna a arquitetura de paredes e janelas amplamente redundante (não obstante firewalls e windows). E ela permite formas de controle que apresentam diferentes faces, que não têm uma conexão óbvia com o aprisionamento e, além disso, amiúde compartilham as características da flexibilidade e da diversão encontradas no entretenimento e no consumo" (BAUMAN, Zygmunt. *Op cit*., p. 8).

[27] George Orwell escreveu o romance distópico 1984. O protagonista Winston conseguia escapar em certos momentos, da vigilância operada pelo Grande Irmão. A teletela era um tipo de tecnologia bidimensional e

uma economia de vigilância em que seus atores têm como modelo de negócio vigiar os cidadãos-potenciais consumidores[28]. A teletela de Orwell é substituída pelas inúmeras microtelas dos aparelhos celulares *smartphones* aos *trackers*[29], numa contínua arquitetura da vigilância[30].

Estabelecido o contexto em que se desenvolve a temática da privacidade e proteção de dados pessoais, passamos a seguir a analisar especificamente o caso da utilização da tecnologia do reconhecimento facial a ser implantada no metrô de São Paulo e a possível violação tanto do direito fundamental a proteção de dados e privacidade, quanto a prerrogativa de atribuição quanto à coleta e seu armazenamento.

Reconhecimento facial e segurança pública: o caso do metrô de São Paulo e o problema da atribuição na coleta e tratamento de dados pessoais

Anteriormente, foram analisadas as problemáticas da implantação de um sistema de reconhecimento facial, notadamente a proteção a ser garantida pelo detentor desse banco de dados, tendo em vista que essas informações devem respeitar os direitos de intimidade e privacidade, bem como deve ser garantida a acurácia do sistema, a fim de se evitar constrangimentos altamente danosos à honra, imagem e autoestima da pessoa, como, por exemplo, já aconteceu no Rio de Janeiro, quando uma mulher foi presa após ser confundida pelo sistema de reconhecimento facial, tendo sido libertada apenas na Delegacia, quando sua verdadeira identidade foi checada[31].

Imagine-se então uma pessoa, acompanhada de seus familiares, amigos ou colegas de trabalho, ser repentinamente detida por forças de segurança estatais, sob alegação de que seria pessoa procurada pela justiça, sendo levada, dependendo da situação, algemada, para uma Delegacia. Ainda que o mal entendido venha a ser desfeito logo depois, obviamente a imagem desta pessoa ficou chamuscada perante seus acompanhantes, isso sem levar em consideração que na sociedade digital atual, e em local extremamente movimentado como o Metrô de São Paulo, muito provavelmente alguém filmará a cena e, em questão de minutos esta imagem, de uma pessoa sendo presa em pleno transporte público, estará em milhares, quiçá milhões de outros celulares, causando danos irreparáveis e de extensão incalculável ao erroneamente reconhecido.

Neste tópico, analisa-se, diante das questões e falhas do sistema analisados anteriormente neste trabalho, o caso do Metrô de São Paulo[32], que em 27 de junho de

fazia as vezes de uma televisão para transmitir as mensagens oficiais do governo e, às vezes, de uma câmera de vigilância para observar os cidadãos em suas residências (BIONI, Bruno Ricardo. op cit., p. 133).

[28] Idem, p. 135.

[29] Referência a todos as ferramentas de rastreamento de hábitos dos consumidores ao longo de sua navegação na internet, como por exemplo os cookies.

[30] BIONI, Bruno Ricardo. *Op cit.*, p. 135.

[31] G1 RIO. *SISTEMA DE RECONHECIMENTO FACIAL DA PM DO RJ FALHA, E MULHER É DETIDA POR ENGANO*. DISPONÍVEL EM HTTPS://G1.GLOBO.COM/RJ/RIO-DE-JANEIRO/NOTICIA/2019/07/11/SISTEMA-DE-RECONHECIMENTO-FACIAL-DA-PM-DO-RJ-FALHA-E-MULHER-E-DETIDA-POR-ENGANO.GHTML. Acesso em 02 jul. 2020.

[32] Importante ressaltar que o Metrô de São Paulo é uma empresa pública estadual, parte integrante da administração indireta, ou seja, é instituição que se submete aos princípios da administração pública como legalidade, impessoalidade, publicidade e eficiência, ostentando desta forma natureza eminentemente

2019 lançou edital para a contratação de sistema de monitoração eletrônica das linhas 1 – azul, 2 – verde e 3 - vermelha da Companhia do Metropolitano de São Paulo[33].

Já em análise superficial, detecta-se a primeira falha, uma vez que o sistema metroviário da cidade de São Paulo, além das três linhas já citadas, ainda é composto pela Linha 4 – Amarela[34], Linha 5 – Lilás[35] e Linha 15 – Prata. As duas primeiras tiveram suas operações concedidas à iniciativa privada, e a última, embora ainda esteja sendo operada pelo ente estatal, também deve ser objeto de concessão[36].

Assim, embora seja um único sistema de transporte, com a livre circulação de passageiros entre as diversas linhas, inclusive de maneira gratuita, apenas em parte do sistema haverá a implantação do sistema de reconhecimento facial. Ainda que no futuro, as concessionárias decidam expandir este sistema de monitoramento, não há qualquer obrigação jurídica que imponha às pessoas jurídicas de direito privado a obediência ao mesmo sistema de coleta, tratamento e, principalmente, proteção dos dados, já que nem no edital de contratação do serviço, nem nos contratos de concessão, há qualquer cláusula determinando a uniformização de sistema de monitoramento eventualmente implantado.

Esta ausência de uniformidade no monitoramento levanta algumas problemáticas, pois existirá um tratamento diferenciado para usuários do mesmo serviço, pois aquele que utiliza as linhas sob operação direta do Metrô, com exceção da linha 15, será monitorado, enquanto o usuário que utiliza as linhas sob concessão não.

Conforme já estudado, a implantação do sistema de reconhecimento facial, decorrente da quarta revolução industrial, parece inafastável. Assim, haverá um momento em que o sistema - atualmente operado por três pessoas jurídicas distintas, mas com grandes possibilidades de serem quatro os *players* - poderá trabalhar com diversos sistemas de monitoramento facial, expondo o usuário à captação da sua imagem por sistemas com índices de acerto distintos e níveis diversos de proteção de seus dados. A melhor solução para o citado problema seria o aditamento dos contratos de concessão, e do edital de concessão da Linha 15, devendo constar nos instrumentos quais os requisitos técnicos que as concessionárias deverão obedecer quando eventualmente implantarem o sistema de reconhecimento facial nas linhas que operam, devendo ainda este dispositivo jurídico conter exigências de nível de acuidade mínima no reconhecimento, quanto a proteção dos dados coletados e o tratamento dado a eles, já que como o executor do serviço público é a iniciativa privada, deve ser coibido o uso destes dados com o intuito de lucro.

administrativa. Suas atribuições não se confundem com a de outras instituições como as de segurança pública, já que tem como finalidade o transporte público.

[33] Edital disponível em https://transparencia.metrosp.com.br/dataset/editais-e-instrumentos-contratuais/resource/726be966-0fb0-46dc-9dd3-dfcce9970a29. Acesso em 05 jul. 2020.

[34] Com operação e exploração dos serviços concedida à Concessionária da Linha 4 do Metrô do Metrô de São Paulo S.A. até 2038, nos termos do Contrato 4232521201. Disponível em http://www.parcerias.sp.gov.br/Parcerias/Documento/Download?codigo=2186. Acesso em 08 jul. 2020.

[35] Idem.

[36] Processo STM 000816/2017 – Concessão Linha 15 Prata. Documento disponível em http://www.parcerias.sp.gov.br/Parcerias/Documento/Download?codigo=29032. Acesso em 08 jul. 2020.

Passa-se agora a analisar a contratação já feita pelo Metrô, para implementação do sistema de reconhecimento facial nas linhas diretamente operadas pela pessoa jurídica de direito público.

Ao definir os critérios de avaliação e qualificação das propostas[37], o Metrô definiu que, para fins de escolha do vencedor (item 2), será utilizado unicamente o critério de menor preço, não fazendo nenhuma exigência de ordem qualitativa, ou seja, não se exige do vencedor qualquer *expertise* na implantação e gestão de sistemas de reconhecimento facial, ou que o licitante comprove possuir capacidade técnica para garantir que os dados coletados protejam a intimidade dos usuários do sistema.

Ainda na mesma seção, ao exigir que o licitante prove documentalmente possuir experiência e capacidade técnica de implementar o sistema de monitoramento (item 4), o Metrô exige apenas que o futuro contratado tenha capacidade de fornecer e implementar o sistema que opere com, no mínimo, 993 (novecentas e noventa e três) câmeras, servidores de alta capacidade para armazenamento de imagens e gerenciamento das imagens das câmeras com no mínimo 2.000 TB (dois mil terabytes); rede de transmissão de dados de, no mínimo 10 Gbps (dez gigabytes por segundos); e sistema integrado com softwares e ferramentas de inteligência artificial.

Ao analisar com maior profundidade o último requisito, já que o coração do sistema de reconhecimento facial, como já visto, é um algoritmo, que por sua vez utiliza algum padrão matemático, é possível perceber que há uma grande diferença no percentual de acerto conforme varia a combinação algoritmo – padrão matemático. O Metrô, ao iniciar o processo de contratação, sequer delimitou o emprego dos algoritmos já conhecidos e cientificamente comprovados como de melhor percentual de acerto, não havendo qualquer óbice, do ponto de vista jurídico, da utilização de sistema com baixo índice de acerto.

Um estudo realizado por Alex Lima Silva e Marcos Evandro Cintra, no qual foi comparada a acurácia de diversos sistemas de reconhecimento facial, obteve, valendo-se de um banco de dados chamado *Brazilian Face Database*, níveis de acerto muito díspares, de acordo com o binômio algoritmo – padrão matemático utilizado. Neste estudo foram testadas dez combinações diferentes. A mais precisa teve 94,32% de acerto, enquanto o pior índice apurado foi de 53,41%[38].

Ainda no Edital, há a publicação de um formulário denominado "planilha de preço", que deve ser preenchido pelo licitante. Ao descrever o software de reconhecimento que deve ser empregado, há tão somente a exigência de um "software analítico de análise forense (software de análise de conteúdo de vídeos) com licenças para cerca de 1500 câmeras e com os servidores necessários para lidar com imagens de 1500 câmeras"[39].

[37] Edital disponível em https://transparencia.metrosp.com.br/dataset/editais-e-instrumentos-contratuais/resource/726be966-0fb0-46dc-9dd3-dfcce9970a29, p. 44-48. Acesso em 05 jul. 2020.

[38] SILVA, Alex Lima; CINTRA, Marcos Evandro. Reconhecimento de padrões faciais**:** Um estudo. In: IFRN. *VII Escolar Potiguar de Computação e suas Aplicações – TI como Fartor de Desenvolvimento Regional*. Santa Cruz – RN, 2014. Disponível em https://pdfs.semanticscholar.org/aa94/f214bb3e14842e4056fdef834a51aecef39c.pdf. Acesso em 25 jun. 2020.

[39] Edital disponível em https://transparencia.metrosp.com.br/dataset/editais-e-instrumentos-contratuais/resource/726be966-0fb0-46dc-9dd3-dfcce9970a29, p. 59, 65, 86 e 98. Acesso em 05 jul. 2020.

Ainda que o ente público não quisesse eleger um algoritmo a ser empregado no software, visando afastar qualquer alegação de direcionamento do processo licitatório, deveria ao menos fixar margem mínima de acerto do processo de reconhecimento facial, bem como estabelecer parâmetros razoáveis de segurança deste software, já que, quando em pleno funcionamento, este sistema gigantesco diariamente captará, tratará e armazenará a imagem de milhões de pessoas[40].

A licitação foi vencida pelo Consórcio Engie Ineo Johnson, formado pelas empresas Engie Brasil Soluções Integradas Ltda, Ineo Infracom e Johnson Controls BE do Brasil, que, ofereceu o menor preço, qual seja, R$ 58.618.282,54 (cinquenta e oito milhões, seiscentos e dezoito mil, duzentos e oitenta e dois reais e cinquenta e quatro centavos) para a implantação do sistema[41].

Analisando o contrato celebrado com o consórcio vencedor, não há qualquer inovação quanto às exigências de ordem técnica em relação ao edital, não prevendo o instrumento qualquer cláusula exigindo excelência no funcionamento do sistema de reconhecimento facial, ou seja, o sistema será de fato implantado pelo contratado sem qualquer norma jurídica que o obrigue a entregar um sistema seguro no tocante à coleta, tratamento e armazenamento dos dados.

Assim, as Defensorias Públicas do Estado de São Paulo e da União, o IDEC – Instituto Brasileiro de Defesa do Consumidor, e as associações civis Intervozes – Coletivo Brasil de Comunicação Social e Artigo 19 Brasil ajuizaram ação de produção antecipada de provas contra o Metrô[42].

O pedido foi deferido pelo Juízo, determinando que o Metrô prestasse uma série de informações, como a eficácia e confiabilidade do sistema; a forma de coleta, tratamento, armazenamento e proteção dos dados coletados; e quais seriam os bancos de dados utilizados para comparação das imagens coletadas.

Em sua resposta, o Metrô, primeiramente, informa que o sistema contratado, prioritariamente será destinado ao mero monitoramento do sistema, alegando que "a identificação facial de pessoas somente será utilizada em casos muito específicos (...) como por exemplo, busca de pessoas desaparecidas, ou identificação de um usuário que eventualmente tenha praticado algum crime nas dependências do Metrô, bem como busca após determinação judicial."[43]

Neste ponto, ao nosso ver, fica evidente que o sistema de reconhecimento facial do Metrô será sim um instrumento utilizado na repressão penal, uma vez que o próprio assume que usará o sistema para identificação de suspeitos pela prática de crimes praticados em suas dependências, bem como utilizará o sistema para efetuar a detenção

[40] Segundo informações do próprio Metrô no mês de fevereiro de 2020, mais de 65 milhões de pessoas utilizaram as linhas 1, 2, 3 e 15. Disponível em <https://transparencia.metrosp.com.br/dataset/demanda/resource/12085898-7e70-46e4-b84b-c0701cb53d2b>. Acesso: 08 jul. 2020.

[41] Contrato 1001455701, celebrado em 13 dez. 2019. Disponível em <https://transparencia.metrosp.com.br/dataset/editais-e-instrumentos-contratuais/resource/726be966-0fb0-46dc-9dd3-dfcce9970a29>. Acesso em 05 jul. 2020.

[42] Processo digital 1006616-14.2020.8.26.0053, em trâmite perante a 1ª Vara da Fazenda Pública do Foro Central da Comarca da Capital/SP. Processo digital, que pode ser consultado junto ao sítio do TJ/SP.

[43] Idem, p. 555.

de pessoas procuradas pela Justiça, pois esta é a única interpretação possível a ser extraída da afirmação acima grifada.

Não havendo dúvidas sobre a utilização do sistema na política de segurança pública e sabendo que o reconhecimento facial trabalha com a comparação do rosto captado em tempo real com um banco de dados prévio, parece evidente que o corpo funcional do Metrô, ou até mesmo os particulares que estarão operando o sistema, já que nem o edital nem o contrato deixam claro quem operará o sistema após a implantação, terão acesso ao banco de dados da Secretaria de Segurança Pública, pois somente este tem a informação de quem são as pessoas que tem ordem de prisão contra si e também é o principal órgão responsável pela identificação civil da população.

Tal situação fere direitos fundamentais tais como: direito à intimidade, privacidade, imagem do usuário e direito a proteção de dados pessoais, pois tais informações não são de domínio público e sequer podem ser requisitadas por algum interessado, sendo de conhecimento exclusivo dos integrantes do sistema de segurança pública, do Ministério Público e do Poder Judiciário. Patente a ilegalidade e/ou inconstitucionalidade.

Ainda na contestação, o Metrô invoca as leis federais n.ºs 6.149/1974 e 5.970/1973 para justificar que seu corpo de segurança possui poder de polícia, "inclusive com atribuições relativas à prisão e lavratura de boletim de ocorrência."[44]

Contudo, não é possível confundir poder de polícia, conceito de direito administrativo[45], com competência legal para investigação criminal, que, nos termos do artigo 4º do Código de Processo Penal e seu parágrafo único, poderá ser exercida somente pela autoridade policial e, excepcionalmente por outras autoridades administrativas cuja lei tenha outorgado tal função.

De pronto, exclui-se da análise a lei 5.970/1973, que versa sobre a possibilidade da não preservação do local de acidente de trânsito, quando tal procedimento foi prejudicial ao tráfego, excluindo a aplicação do artigo 6º, inciso I, do Código de Processo Penal[46] nestas hipóteses.

Já a lei 6.149/1974, em seu artigo 3º, determina que o serviço de transporte deverá "manter corpo próprio e especializado de agente de segurança" que tem como uma de suas funções básicas "a preservação do patrimônio vinculado", conforme disposto no artigo 2º.

O artigo 4º da mesma lei estabelece que este corpo próprio de segurança deverá colaborar com a Polícia local para manter a ordem pública, prevenir ou reprimir crimes e

[44] Processo digital 1006616-14.2020.8.26.0053, em trâmite perante a 1ª Vara da Fazenda Pública do Foro Central da Comarca da Capital/SP. Processo digital, que pode ser consultado junto ao sítio do TJ/SP, p. 556.
[45] Que segundo Hely Lopes Meirelles "é a faculdade de que dispõe a Administração Pública para condicionar e restringir o uso, o gozo de bens, atividades e direitos individuais, em benefício da coletividade ou do próprio Estado. O Poder de polícia é o mecanismo de frenagem de que dispõe a Administração Pública para conter os abusos do direito individual" (MEIRELLES, Hely Lopes. *Direito Administrativo Brasileiro*. São Paulo: Malheiros, 1999. p. 115).
[46] Art. 6º Logo que tiver conhecimento da prática da infração penal, a autoridade policial deverá: I - dirigir-se ao local, providenciando para que não se alterem o estado e conservação das coisas, até a chegada dos peritos criminais (BRASIL. Código de Processo Penal. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/del3689compilado.htm. Acesso em: 20 jul 2020).

contravenções penais nas áreas do serviço de transporte metroviário. Ou seja, não há qualquer autorização legal para que o corpo de segurança do Metrô atue na repressão penal, devendo, tão somente, auxiliar os órgãos investigativos, o que implica no reconhecimento de mais uma ilegalidade/inconstitucionalidade.

Quanto à realização de prisões por parte dos prepostos do Metrô, o inciso II do mesmo artigo 4º os autoriza a "prender em flagrante os autores dos crimes ou contravenções penais e apreender os instrumentos e os objetos que tiverem relação com o fato, entregando-os à autoridade policial competente". Entretanto, a prisão em flagrante é facultada a qualquer do povo, nos termos do artigo 301 do Código de Processo Penal, o que não pode ser confundido com a prisão em razão de mandado judicial, que só pode ser realizada por integrantes do sistema de segurança pública.

Ainda na demanda judicial, o Metrô alega que o sistema de reconhecimento facial não estará sujeito às disposições da LGPD, uma vez que "a coleta de dados (...) estará ligada à Segurança Pública e/ou atividades de investigação e repreensão a infrações penais", invocando o artigo 4º, inciso III, alíneas a) e d) da LGPD.[47] Trata-se, aqui, de outro claro equívoco. Isso porque o conceito de "dado pessoal" não envolve apenas informações, notadamente escritas, mas sim a toda e qualquer informação que, relacionada à uma pessoa natural, seja capaz de identificá-la. Dessa forma, "a imagem de uma pessoa, por exemplo, é dado pessoal, desde que seja possível identificá-la. Isso se aplica tanto a fotos quanto a vídeos[48]".

Ademais, seja por meio de uma imagem ou de um vídeo, outras informações relevantes e atinentes às pessoas podem ser extraídas, de modo que "identificar uma pessoa não quer dizer necessariamente saber seu nome, endereço, telefone, etc. Trata-se de identificar no sentido de individualizar uma pessoa num grupo social[49]. Dessa forma:

> [...] Uma fotografia ou um vídeo que mostra uma pessoa rezando dentro de uma igreja, ou participando de um partido político, torna possível identificar a religião e as opiniões políticas dessa pessoa.
> No exemplo mencionado no parágrafo anterior, o problema se torna ainda mais complexo, uma vez que informações relacionadas a convicções religiosas e opiniões políticas são consideradas pela LGPD "dados pessoais sensíveis". Essa espécie de dado pessoal recebe uma proteção ainda maior da lei e seu tratamento exige um cuidado especial por parte das pessoas físicas e jurídicas que o tratam[50].

Dessa forma, enquadrando-se como empresa que lidará com o tratamento de dados de milhões de pessoas, o Metrô fatalmente estará submetido aos termos da LGPD brasileira, devendo observância aos comandos e princípios estatuídos pela legislação, notadamente aos requisitos exigidos pelo artigo 7º da mencionada Lei para o tratamento

[47] Art. 4º. Esta Lei não se aplica ao tratamento de dados pessoais: (...) III – realizado para fins exclusivos de: a) segurança pública; (...) d) atividades de investigação e repressão de infrações penais (BRASIL. Lei Geral de Proteção de Dados. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 20 jul. 2020)

[48] LOPES, Marcelo Frulanni. A lei geral de proteção de dados pessoais e o direito de imagem. *JOTA* [online], 2019.

[49] BARBOSA, Danilo Ricardo Ferreira; SILVA, Carlos Sérgio Gurgel da. A coleta e o uso indevido de dados pessoais: um panorama sobre a tutela da privacidade no Brasil e a lei geral de proteção de dados. *RJLB*, ano 5, n. 6, 2019. p. 493.

[50] LOPES, Marcelo Frulanni. *Op cit.*, 2019.

de dados – dentre eles o consentimento do titular -, sob pena de sofrer a aplicação de penalidades altíssimas no caso de seu descumprimento.

Assim, para tentar elidir-se da responsabilidade imposta pela *novel* legislação, o Metrô reafirma, de maneira totalmente equivocada, que seu sistema de reconhecimento facial será ferramenta de execução de políticas de segurança pública, sendo que, como já provado, não há qualquer autorização legal para que seu corpo de segurança atue nesta seara, não podendo, a nosso ver, ter acesso a dados sigilosos ligados à segurança pública.

Assim, entende-se que a única solução viável para a utilização do sistema de reconhecimento facial na segurança pública seria a implantação do caminho inverso. O Metrô, através de um consórcio, cederia acesso ao seu sistema aos órgãos de segurança pública que, de forma interna e com seu corpo funcional, trabalharia essas imagens a fim de identificação de criminosos.

Ratificando o entendimento já exposto, relevante mencionar que a tecnologia de captação dos rostos dos usuários já foi utilizada em parte do sistema metroviário de transporte, a Linha 4 Amarela, que instalou painéis digitais nas portas de entrada e saída das composições veiculando publicidades diversas, e junto dessas, câmeras que captavam o rosto das pessoas que assistiam a esses comerciais. A concessionária visava criar um banco de dados capaz de aumentar sua lucratividade com a cessão de espaços para publicidade, pois poderia oferecer um mapeamento completo a potenciais clientes. Tal desiderato valer-se-ia das informações dos usuários do transporte como: o número de usuários em cada período do dia, a idade média deles, cor/raça e até mesmo a reação das pessoas conforme o comercial exibido.

A legalidade da implantação desta tecnologia foi questionada judicialmente pelo Instituto de Defesa do Consumidor – IDEC, que ajuizou a ação civil pública 1090663-42.2018.8.26.0100, com trâmite perante a 37ª Vara Cível do Foro Central da Comarca da Capital/SP. De plano foi concedida tutela antecipada determinando a cessação da captação das imagens dos usuários, com o desligamento das câmeras e ainda a colocação de adesivos nas lentes.

A concessionária impugnou o pleito alegando que o sistema utilizado não era de reconhecimento facial, não identificava as pessoas, mas apenas de "detecção de rostos classificáveis em categorias de expressões, gêneros e tipos"[51]. Também alegou que os

[51] TJSP. *Ação Civil Pública nº 1090663-42.2018.8.26.0100*, p. 2283. Disponível em: https://esaj.tjsp.jus.br/cpopg/show.do;jsessionid=9E55E08EBCA5A52D49C0854CE2B7A751.cpopg8?conversationId=&cbPesquisa=NUMPROC&numeroDigitoAnoUnificado=1090663-42.2018&foroNumeroUnificado=0100&dadosConsulta.valorConsultaNuUnificado=10906634220188260100&dadosConsulta.valorConsultaNuUnificado=UNIFICADO&dadosConsulta.valorConsulta=&dadosConsulta.tipoNuProcesso=UNIFICADO&uuidCaptcha=sajcaptcha_e3ab9b92da0643aba1837e2ac5a5a377&g-recaptcha-response=03AGdBq26Ni5Jw7QUPxCXO_XUmsE8gmTcGk_wCyAsnCY7Y8DIRh0XtGi1S7aZXHBCcPM2Xuvun6j13hpVu1_TvSMeLfuG0lMEFOM5YWl1rlWxRa02Yrlz3Nes6F3kE7CpYpXVx_RMWwdYDdqGgJxnszTSY8Vo6oLfUI1LtN-_AGIdkkEQbOCklOLlA6XRERllTTR-XSUbxxzriJ1ry8Ws0ONwCMr5nIqTmTzgn5MO33qmaY2QKHdxeMvsEHHTGE1yzPz9kdGvP1Hf-Z4kJMGqD7QgS1Nd-_NRLfeCBHj_MSu7UyrxWjvptc6ebMnJv_APRt893uzOSYUJXBOZysajZmkv9Zzi3OeYJeCzpaQIEFa2t9TxTxmIkzPEzREb3d2KceCRy1BqJ1HEGrHYLUES4Iu8nj_DrcQ2c1k3nNwrZf4YLH-cRupQt9m1zEeYbKl52-eXlRk_F2mukyLBkNVkkPMNh8bGPi3nWcw&processo.codigo=2S000WSPS0000. Acesso em 7 jun. 2021.

dados não eram tratados e armazenados, sendo a coleta somente para fins estatísticos. Por fim, afirmou que tinha autorização do poder concedente para a implantação da tecnologia.

O processo, acertadamente, foi julgado parcialmente procedente, confirmando a tutela antecipada e condenando a ré no pagamento de danos morais coletivos no valor de cem mil reais. No início da fundamentação, o Juízo invoca o art.11, I da LGPD, já que a concessionária captava as imagens sem autorização do usuário, não ficando comprovada nenhuma das hipóteses previstas no inciso II do mesmo artigo, que dispensa a autorização para tratamento dos dados, pois a mera detecção facial, procedimento alegado pela ré, já deve ser considerado dado biométrico e, consequentemente dado sensível.

Além disso, a concessionária sequer informava os usuários que seus rostos, feições e reações estavam sendo captados, em flagrante desrespeito ao artigo 6º, III e IV da Lei 8.078/1990 – CDC.

Também foi refutado acertadamente a alegação que a concessionária tinha autorização do Poder Público, corroborando o Juízo o entendimento do Ministério Público que "É irrelevante a anuência do Metrô, porque o ato permanece sendo ilegal, porque o Estado não pode dispor dos direitos fundamentais dos cidadãos e, diversamente do alegado pela ré, esta exploração econômica em absolutamente nada interfere na garantia da modicidade dos preços das tarifas, porque reverte o lucro exclusivamente em favor da ViaQuatro"[52].

Por fim, o Juízo afastou a alegação da Via Quatro de que os dados não eram tratados e armazenados, pois a própria ré não conseguiu demonstrar, durante todo o plexo probatório, que não realizava determinadas atividades.

Esta alegação da ré nos parece totalmente inverossímil, pois se o objetivo da Via Quatro era justamente criar um *big data* de seus usuários visando justamente oferecer no mercado a possibilidade de veiculação de publicidades direcionadas, pautadas em um levantamento de seus usuários, identificando individualidades como cor, raça, idade e gênero, bem como seus gostos pessoais, já que captava a reação das pessoas após a exposição delas, parece-nos impossível o não tratamento e armazenamento dessas informações para fins de atingimento do objetivo pleiteado.

[52] TJSP. *Ação Civil Pública nº 1090663-42.2018.8.26.0100*, p. 2292. Disponível em: https://esaj.tjsp.jus.br/cpopg/show.do;jsessionid=9E55E08EBCA5A52D49C0854CE2B7A751.cpopg8?conversationId=&cbPesquisa=NUMPROC&numeroDigitoAnoUnificado=1090663-42.2018&foroNumeroUnificado=0100&dadosConsulta.valorConsultaNuUnificado=10906634220188260100&dadosConsulta.valorConsultaNuUnificado=UNIFICADO&dadosConsulta.valorConsulta=&dadosConsulta.tipoNuProcesso=UNIFICADO&uuidCaptcha=sajcaptcha_e3ab9b92da0643aba1837e2ac5a5a377&g-recaptcha-response=03AGdBq26Ni5Jw7QUPxCXO_XUmsE8gmTcGk_wCyAsnCY7Y8DIRh0XtGi1S7aZXHBCcPM2Xuvun6j13hpVu1_TvSMeLfuG0lMEFOM5YWl1rlWxRa02Yrlz3Nes6F3kE7CpYpXVx_RMWwdYDdqGgJxnszTSY8Vo6oLfUI1LtN-_AGIdkkEQbOCklOLlA6XRERllTTR-XSUbxxzriJ1ry8Ws0ONwCMr5nIqTmTzgn5MO33qmaY2QKHdxeMvsEHHTGE1yzPz9kdGvP1Hf-Z4kJMGqD7QgS1Nd-_NRLfeCBHj_MSu7UyrxWjvptc6ebMnJv_APRt893uzOSYUJXBOZysajZmkv9Zzi3OeYJeCzpaQIEFa2t9TxTxmIkzPEzREb3d2KceCRy1BqJ1HEGrHYLUES4Iu8nj_DrcQ2c1k3nNwrZf4YLH-cRupQt9m1zEeYbKl52-eXlRk_F2mukyLBkNVkkPMNh8bGPi3nWcw&processo.codigo=2S000WSPS0000. Acesso em: 7 jun. 2021.

CONSIDERAÇÕES FINAIS

Diante do exposto, entende-se que a quarta revolução industrial já está em andamento, e que um de seus vetores, a implantação em larga escala de sistemas de reconhecimento facial é inafastável, devendo cada vez mais fazer parte do cotidiano de todos nós.

Assim, é natural e até mesmo salutar que o meio de transporte mais movimentado no país utilize tal tecnologia, visando aumentar o nível de proteção de seu patrimônio, o resguardo à incolumidade física de seus milhões de usuários, fatores que são decisivos para um melhor funcionamento do sistema.

Embora seja iniciativa que dialoga com os novos tempos que em se vive, preocupa a forma como a implantação e gerenciamento do sistema será feito, pois como se estudou, em nenhum momento de todo o processo licitatório o Metrô fez qualquer exigência de ordem técnica visando colocar em funcionamento um sistema que seja seguro o suficiente para garantir que os dados coletados, contendo a biometria facial de milhões de pessoas, não sofra qualquer desvio de finalidade, como, por exemplo, a utilização comercial desta gigantesco bloco de informações.

Também se verificou que o Metrô, em nenhum momento, criou qualquer obrigação jurídica com o consórcio contratado exigindo um percentual mínimo de acerto do sistema de reconhecimento, já que é cientificamente comprovado que, de acordo com o algoritmo e o sistema matemático utilizados, o nível de acerto é oscilante.

Além de não prever tais requisitos técnicos, o Metrô informou que seu sistema de reconhecimento facial será usado como política de segurança pública, o que fere direitos e garantias fundamentais, configurando ilegalidades e inconstitucionalidades.

Primeiro, porque o Metrô não integra o sistema de segurança pública, composto exclusivamente pelas instituições listadas no rol taxativo previsto no artigo 144 da Constituição Federal. Assim, parece violação ao direito à privacidade o atuar do Metrô, como explicitamente afirmou na ação judicial n. 1006616-14.2020.8.26.0053 em tela estudada, que o sistema de reconhecimento facial seja utilizado para a detenção de pessoas com a ordem judicial de prisão em aberto, uma vez que para execução deste ato, obviamente deverá possuir banco de dados contendo o rol de todas as pessoas nesta situação, bem como toda a sua qualificação, informações que devem ser de conhecimento exclusivo dos atores da persecução penal – polícias, Ministério Público e Poder Judiciário, não havendo possibilidade que tais dados sejam cedidos ainda que celebrado convênio entre as instituições.

Segundo que o corpo de segurança do Metrô, a despeito do afirmado na citada ação judicial, não possui qualquer autorização legislativa para investigação, tendo como competências funcionais a defesa do patrimônio, da proteção do usuário e a cooperação com os verdadeiros órgãos de investigação.

Por fim e não menos importante, deve-se chamar atenção para os flagrantes riscos advindos do fato de se dispor/delegar à iniciativa privada a possibilidade de exploração de tecnologia de reconhecimento facial, mesmo que para fins "justificáveis", uma vez que o controle sobre a real utilização desses dados pessoais – que podem inclusive ser

caracterizados como sensíveis a depender do contexto de captura da imagem ou vídeo – será inexistente ou mínimo, o que pode acabar gerando episódios de divulgação massiva de dados pessoais para fins exclusivamente comerciais ou econômicos, sem o consentimento dos titulares; o que não pode e não deve ser admitido.

Portanto, caso o governo estadual queira efetivamente utilizar o sistema como política de segurança pública, o que deve ser feito com cautela, pois como viu-se esta tecnologia pode ser imprecisa e até mesmo acentuar erros de identificação, deve o Metrô conceder acesso ao seu sistema, em tela estudado, para que os órgãos de investigação estatal possam, com o banco de dados que possui, e que deve permanecer sigiloso, ampliar a efetividade de sua atuação.

Do mesmo modo, é extremamente importante que o Metrô adote todas as medidas exigidas pela LGPD para o tratamento e segurança desses dados – especialmente a requisição de consentimento dos titulares -, de modo a evitar vazamentos indevidos ou mesmo a utilização para outras finalidades, sob pena de incidência nas penalidades previstas pela legislação correspondente.

REFERÊNCIAS

ABBAS DA SILVA, L.; FRANQUEIRA, B. D.; HARTMANN, I. A. O que os olhos não veem, as câmeras monitoram: reconhecimento facial para segurança pública e regulação na América Latina. *Revista Digital de Direito Administrativo*. [S. l.], v. 8, n. 1, p. 171-204, 2021. DOI: 10.11606/issn.2319-0558.v8i1p171-204. Disponível em: https://www.revistas.usp.br/rdda/article/view/173903. Acesso em 14 fev. 2022.

BARBOSA, Danilo Ricardo Ferreira; SILVA, Carlos Sérgio Gurgel da. A coleta e o uso indevido de dados pessoais: um panorama sobre a tutela da privacidade no Brasil e a lei geral de proteção de dados. *RJLB*, ano 5, n. 6, 2019.

BAUMAN, Zygmunt**.** *Vigilância Líquida:* diálogos com David Lyon. Tradução de Carlos Alberto Medeiros. Rio de Janeiro: Zahar, 2014.

BAUMAN, Zygmunt. *Modernidade Líquida*. Ed. Zahar, 2001.

BECK, Cesar Augusto Moacyr Rutowitsch; BOFF, Murilo Manzoni; PIAIA, Thami Covatti. Os (ab) usos da tecnologia de reconhecimento facial na segurança pública e na prestação de serviços a partir da pandemia de COVID-19. *Revista Pensamento Jurídico*. São Paulo, v. 15, n. 2, ma./ago. 2021.

BIONI, Bruno Ricardo. *Proteção de dados pessoais:* a função e os limites do consentimento. 2ª ed. Rio de Janeiro: Forense, 2020.

BRASIL. *Código de Processo Penal*. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/del3689compilado.htm. Acesso em: 20 jul 2020.

BRASIL. *Lei Geral de Proteção de Dados*. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 20 jul. 2020.

BRASIL. Emenda Constitucional nº 115, de 10 de fevereiro de 2022. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/Emendas/Emc/emc115.htm. Acesso em: 14 fev. 2022.

BRASIL. Câmeras de reconhecimento facial vão ajudar a identificar criminosos no carnaval. *Correio da Bahia***,** Salvador, 26 fev. 2019. Disponível em: https://www.correio24horas.com.br/noticia/nid/cameras-de-reconhecimento-facial-vao-ajudar-a-identificar-criminosos-no-carnaval/. Acesso em: 10 jul. 2020.

CONCEIÇÃO, *Valdir Silva; NUNES, Edna Maria; ROCHA, Ângela Machado.* O Reconhecimento Facial como uma das Vertentes da Inteligência Artificial (IA): um estudo de prospecção tecnológica. *Cadernos de Prospecção***.** Salvador, v. 13, n. 3, p. 745-758, junho, 2020.

G1 RIO. *Sistema de reconhecimento facial da PM do RJ falha, e mulher é detida por engano***.** Disponível em: https://g1.globo.com/rj/rio-de-janeiro/noticia/2019/07/11/sistema-de-reconhecimento-facial-da-pm-do-rj-falha-e-mulher-e-detida-por-engano.ghtml. Acesso em 02 jul. 2020.

GAMBA, João Roberto Gorini**.** *Democracia e tecnologia*: impactos da quarta revolução industrial. Rio de Janeiro: Lumen Juris, 2020.

LOPES, Marcelo Frulanni. A lei geral de proteção de dados pessoais e o direito de imagem. *JOTA* [online], 2019.

MEIRELLES, Hely Lopes. *Direito Administrativo Brasileiro*, São Paulo: Malheiros, 1999.

MORAIS DA ROSA, Alexandre. A questão digital: o impacto da inteligência artificial no Direito. *Revista de Direito da Faculdade Guanambi*, Guanambi, v. 6, n. 02, e259, jul./dez. 2019. doi: https://doi.org/10.29293/rdfg.v6i02.259. Disponível em: http://revistas.faculdadeguanambi.edu.br/index.php/Revistadedireito/article/view/259. Acesso em: 12 jul. 2020.

RODOTÁ, Stefano. *A vida na sociedade da vigilância* – a privacidade hoje. Organização, seleção e apresentação de Maria Celina Bodin de Moraes. Tradução: Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008.

SCHWAB, Klaus. *A quarta revolução industrial*. Tradução Daniel Moreira Miranda. São Paulo: Edipro, 2016.

SILVA, Alex Lima; CINTRA, Marcos Evandro. Reconhecimento de padrões faciais**:** Um estudo. In: IFRN. *VII Escolar Potiguar de Computação e suas Aplicações – TI como Fartor de Desenvolvimento Regional*. Santa Cruz – RN, 2014. Disponível em https://pdfs.semanticscholar.org/aa94/f214bb3e14842e4056fdef834a51aecef39c.pdf. Acesso em 25 jun. 2020.

SILVA, Rosane Leal da; SILVA, Fernanda dos Santos Rodrigues da. Reconhecimento facial e segurança pública: os perigos do uso da tecnologia no sistema penal seletivo brasileiro. *Anais do 5º Congresso Internacional de Direito e Contemporaneidade*: mídias e direitos da sociedade em rede. UFMS – Universidade Federal de Santa Maria, 2019.

THOMPSON, Isobel. The future of your face. *Life*, 25 jun. 2019. Disponível em: https://theface.com/life/the-future-of-your-face. Acesso em: 12 jul. 2020.

VIANA, Cleiton Correia; CONCEIÇÃO, Valdir Silva; ROCHA, Ângela Machado. Reconhecimento Facial e a Relativização do Direito da Imagem**.** *REVISTA INGI***.** Vol.3, n.3, p.436-450. Jul/Ago/Set, 2019. Disponível em: http://ingi.api.org.br/index.php/INGI/article/view/50. Acesso em: 11 jul. 2020.

Data de Recebimento: 20/09/2021.
Data de Aprovação: 17/04/2022.