

O reconhecimento biométrico facial e a utilização pelo Poder Público

Facial biometric recognition and the use by Public Authorities

Kátia Shimizu de Castro¹

Luciana Veiga de Paula²

RESUMO

A biometria facial vem sendo cada vez mais utilizada pelo poder público para reconhecimento dos indivíduos. Apesar dos dados biométricos faciais serem considerados sensíveis, o uso desta tecnologia carece de cuidado no que tange ao direito à privacidade e aos possíveis casos de vieses discriminatórios capazes de trazerem aos seus titulares danos irreparáveis, vez que acontecimentos nessa esfera são constantemente relatados em países que adotaram o uso dessa tecnologia. No Brasil não existe uma legislação específica que regulamente o seu uso, há projetos de lei há anos em tramitação sem que haja, entretanto, qualquer avanço em sua aprovação, no entanto, apesar da lacuna legislação o poder público faz uso constante do reconhecimento facial.

Palavras-chave: Reconhecimento Biométrico Facial, Direito, Tecnologia, Legislação Poder Público, Transparência, Direitos Fundamentais.

ABSTRACT

Facial biometrics has been increasingly used by the government to recognize individuals. Despite facial biometric data being considered sensitive, the use of this technology requires care with regard to the right to privacy and possible cases of discriminatory biases capable of bringing irreparable harm to their holders, since events in this sphere are constantly reported in countries that adopted the use of this technology. In Brazil there is no specific legislation that regulates its use, there are bills for years in the pipeline without, however, any progress in its approval, however, despite the gap in legislation, the public power makes constant use of facial recognition.

Keywords: Facial Biometric Recognition, Law, Technology, Public Power Legislation, Transparency, Fundamental Rights.

¹ Mestranda em Direito Civil Comparado pela Pontifícia Universidade Católica de São Paulo – PUC/SP. Pós Graduada em Direito e Tecnologia pela Universidade de São Paulo – USP. Bacharel em Direito pela Faculdade de Direito de São Bernardo do Campo – SP. Advogada. katiastcastro@gmail.com

² Pós Graduada em Direito e Tecnologia pela Universidade de São Paulo – USP. Advogada. Lucianaveigadepaula@gmail.com

SUMÁRIO

Introdução. 1. O poder público e a utilização dos dados pessoais; 2. Dos projetos de leis em trâmite no legislativo nacional 2.1. Projeto de lei nº 9.414/2017; 2.2. Projeto de lei nº 9.736/2018; 2.3. Projeto de lei nº 4.612/2019; 2.4. Projeto de lei nº 1.515/2022; 3. Abordagem internacional sobre o reconhecimento facial e seus vieses; 3.1. Europa; 3.2 Estados Unidos; 3.3. China. Conclusão; Referências.

INTRODUÇÃO

A internet trouxe ao mundo uma gigantesca aceleração na evolução tecnológica. Esta evolução está presente em todos os campos de conhecimento e impacta toda a humanidade.

No entanto, à medida que novas tecnologias surgem são necessárias adaptações na rotina dos indivíduos. Comumente referidas adaptações ou readaptações acontecem de forma gradual, em ritmo contínuo, raras vezes acontecem mudanças abruptas, como vivenciamos recentemente em razão da pandemia mundial.

Todas essas inovações, no entanto, devem observar limites a fim de que não haja invasão ou até mesmo supressão dos direitos individuais dos cidadãos.

Para regular o uso destas tecnologias, em maio de 2018 a União Europeia trouxe a GDPR (*General Data Protection Regulation*), essa lei regula o tratamento a ser dispensado pelas empresas aos dados dos indivíduos. Essas regras que incluem a forma de coletar, processar, compartilhar e resguardar os dados pessoais, devem ser seguidas por todas as empresas independente do porte ou área de atuação.

Na sequência do regulamento europeu, o Brasil editou a LGPD (Lei Geral de Proteção de Dados) que possui o mesmo objetivo da GDPR.

Ambas as leis possuem grandes semelhanças tendo como objetivo proteger os direitos fundamentais de liberdade e de privacidade bem como a livre formação da personalidade de cada indivíduo.³

Pois bem, quando se trata de proteger os direitos fundamentais de privacidade de cada indivíduo encontramos uma grande dicotomia na proteção deste direito quando a utilização dos dados se dá pelo poder público.

³ <https://www.gov.br/cidadania/pt-br/aceso-a-informacao/lgpd> acessado em 11 de dezembro de 2022

Se, de um lado, os dados sensíveis só podem ser utilizados com a permissão individual no que concerne a sua aplicação no âmbito privado, por outro, o poder público os utiliza de forma indiscriminada e sem qualquer conhecimento ou autorização argumentando que o interesse público é superior ao individual.

Outro problema reside no tratamento e utilização dos dados coletados, vez que referidas informações biométricas são utilizados para alimentar banco de dados que também tem a finalidade de proceder o aprendizado da máquina, entretanto, não são raros os relatos de vieses discriminatórios, que quando ocorrem afetam o indivíduo, causando danos irreparáveis.

Há relatos mundiais de sistemas que apesar de apresentarem grande grau de eficiência, tiveram grande porcentagem de erro. A preocupação é portanto, que o poder público, antes de fazer uso dessa tecnologia resguarde e evite quaisquer possibilidades de equívocos e prejuízos.

1. O PODER PÚBLICO E A UTILIZAÇÃO DOS DADOS PESSOAIS

Quanto a utilização da tecnologia de reconhecimento facial pelo Poder Público, são inúmeras as aplicações.

A possibilidade de se identificar pessoas em locais públicos hoje é uma realidade mundial, inclusive em nosso país, vez que é ampla a utilização de câmeras em ruas, transportes coletivos, estabelecimentos comerciais e prestadoras de serviços públicos e particulares.

Como já descrito cada captura de imagem de face humana gera uma identidade biométrica que fica armazenado em uma base de dados.

Ocorre que, como dito há uma lacuna legislativa importante no que concerne a utilização de referidos dados sensíveis pelo Poder Público, mesmo quando o objetivo é prover a Segurança Pública.

Com efeito tal lacuna permite que esses dados sejam capturados, armazenados, tratados e sofram uma destinação sem que haja qualquer tipo de fiscalização sobre o seu uso e sobre os cuidados dispensados aos mesmos.

Ocorre que, a Lei Geral de Proteção de Dados excluiu de seu regramento a utilização e os direitos resguardados aos dados sensíveis quando estes forem

utilizados para fins de Segurança Pública, deixando ao encargo do legislativo a elaboração de uma norma competente e específica.

Com a promulgação da Emenda Constitucional nº 115/2022, que acrescentou o inciso LXXIX ao artigo 5º da Constituição, o direito à proteção geral de dados foi alçado a nível de direito fundamental, "a ser assegurado nos termos da lei".

Já a LGPD em seu artigo 4º, caput, III, "a" e "d", c/c §1º, expressa a necessidade de que haja a elaboração de uma "lei específica que deverá prever medidas proporcionais e estritamente necessárias ao atendimento do interesse público, observados o devido processo legal, os princípios gerais de proteção e os direitos do titular".

Ainda no que se refere aos demais usos pelo Poder Público de referidos dados pessoais, veja que carece também de regulamentação a utilização da identificação biométrica âmbito de investigação e persecução penal, revelando-se urgente uma norma constitucional sobre o tema.

Dessa forma, como inexistente uma lei que verse sobre a sua utilização revela-se concluído ser temerária a utilização de dados pelo poder público, ainda mais sem que haja qualquer conhecimento ou autorização de seu titular.

2. DOS PROJETOS DE LEIS EM TRÂMITE NO LEGISLATIVO NACIONAL

Existem quatro projetos de lei em tramitação na Câmara dos Deputados, que versam sobre a utilização da biometria facial. Cada um deles com um enfoque diferente e que versam sobre colisão de direitos e deveres distintos entre si.

2.1 Projeto de lei nº 9.414/2017

Esse projeto⁴ que versa sobre a instalação de câmeras em veículos e estações de transporte públicos coletivos, possui como ementa:

"Obriga a instalação da leitura de impressão digital e facial nos meios de transportes público coletivos".

⁴ Projeto de Lei nº 9.414/2017. https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=1634793 acessado em 12/12/2022

Na verdade, essa lei tem a finalidade de tornar possível através de câmeras a autenticidade da identidade do usuário do transporte público, impedindo a ocorrência de fraudes com a utilização de benefícios oriundos a determinado seguimento da população, como por exemplo, passe a estudantes. No teor da justificativa do projeto retro citado a Deputada Mariana Carvalho explica que:

“No projeto, uma câmera seria unida ao validar com o objetivo de comprovar se o dono do cartão é quem realmente está o utilizando. O equipamento é capaz de fazer o reconhecimento de 20 pontos do rosto em frações de segundos, tirando de cinco a dez fotos do passageiro. Caso o sistema identifique que o passageiro não é o dono do cartão, o bilhete não será aceito na próxima viagem e o usuário será chamado a prestar explicações”.

Ressalta-se que o sistema de identificação abordado pelo projeto citado, trata de um meio de autenticação, ou seja, quando da emissão do documento a ser utilizado no transporte público, haverá a captura da biometria facial, sendo essa armazenada em um banco de dados que servirá de base para a comparação quando o usuário fará uso do transporte público.

Veja, nesse caso, há uma vigilância não só quanto a identidade do usuário do transporte, como também o trajeto que foi percorrido por ele. Dessa forma, esbarramos, mais uma vez, no armazenamento e análise de dados que podem trazer uma mitigação quanto a alguns direitos fundamentais, como a privacidade, intimidade e a liberdade do indivíduo.

2.2 Projeto de lei nº 9.736/2018

Esse projeto⁵ de lei é uma proposta de acréscimo a Lei de Execuções Penais, com a finalidade da formação de um banco de dados daqueles que integram o sistema prisional, permitindo a identificação e o acompanhamento daqueles que em algum momento estiveram recolhidos ao sistema carcerário brasileiro.

O deputado Júlio Lopes, ressalva que: “A presente proposta tem por objetivo tornar obrigatória a identificação biométrica de custodiados pelo Estado pelo método de reconhecimento facial. Com o aumento da população no Brasil, o sistema de

⁵ Projeto de Lei nº 9.736/2018.
https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=1643053&filename=P L+9736/2018 acessado em 12/12/2022

identificação civil, usado para fins de identificação criminal, precisa ser aperfeiçoado. Tal medida se justifica pela necessidade do aumento da segurança nos estabelecimentos penais, o que segue uma tendência mundial”.

Nesse quesito a proposta prevê a criação de um banco de dados de identificação de detentos. Temos como consequência, portanto, a criação de um banco de dados de ex- detentos, sem que haja, entretanto, qualquer menção sobre o tratamento e o armazenamento desses dados.

2.3 Projeto de lei nº 4.612/2019

Esse projeto⁶ de autoria do Deputado Bibó Nunes, propõe a criação de um marco regulatório para o uso dessa tecnologia de reconhecimento facial no território nacional. O teor desse projeto é o que mais interessa dentro da exposição do presente estudo, sem, entretanto, trazer as respostas necessárias para a resolução de impasses presentes no uso da tecnologia ora analisada.

Com efeito sua ementa, discorre que:

“Dispõe sobre o desenvolvimento, aplicação, uso de tecnologias de reconhecimento facial e emocional, bem como outras tecnologias digitais voltadas à identificação de indivíduos e a predição e análise de comportamentos”.

Dentre as justificativas estão que:

“Assim, o desenvolvimento e uso de tais tecnologias demanda regulamentação para garantir proteção dos cidadãos contra atos de discriminação e deturpação de seus usos. Urge que preservemos a privacidade do cidadão e defendamos as suas liberdades. Exceto ser por interesse única e exclusiva do Estado”.

Ocorre que, o disposto nesse projeto de lei, visa regulamentar os limites da exposição e a utilização de dados sensíveis. Um ponto bastante importante é que o projeto de lei inclui tornar lícito além da identificação dos indivíduos a sua análise comportamental, é o caso por exemplo do litígio entre o IDEC – Instituto Brasileiro

⁶ Projeto de Lei nº 4.612/2019.
https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=1794019&filename=P L+4612/2019 acessado em 12/12/2022

de Defesa do Consumidor e a ViaQuatro, empresa concessionária da linha 4 – amarela do metro de São Paulo.

A questão trata de uma ação civil pública⁷ em que o IDEC move em face da concessionária, para que, em suma, a empresa se abstenha de utilizar portas interativas em suas estações.

Ocorre que em abril de 2018, a empresa concessionária instalou em algumas de suas estações portas interativas digitais fazendo com que, enquanto os usuários aguardassem o embarque, assistissem campanhas publicitárias ali veiculadas. Com isso foi possível através de câmeras identificar o passageiro, ou seja, seu gênero, idade, além de também identificar suas reações e emoções como entusiasmo, surpresa, tristeza.

Esses dados foram armazenados com a informação de localização e horário da captação da imagem biométrica. Na ação o IDEC alegou que a ViaQuatro coletou dados sem que houvesse qualquer consentimento dos passageiros, levantando, ainda a hipótese de uma possível comercialização dessas informações, requereu, portanto, o desligamento das câmeras e o pagamento de uma indenização por danos coletivos.

Algumas questões bastante pertinentes foram levantadas nessa demanda. Primeiro, como já vimos no decorrer da presente explanação, os dados biométricos faciais, são considerados, pela lei, como dados sensíveis, sendo assim, a sua captação, tratamento e armazenamento sujeito as regras impostas pela lei. É esse o ponto central de divergência da lide.

Ocorre que, não foram observados pela concessionária pontos cruciais ao direito do usuário e a preservação de seus dados pessoais, sequer foi informado previamente de que dados ali estavam sendo coletados. Nesse mesmo sentido se manifestou o Ministério Público⁸ nos autos ao afirmar que:

“A captação de dados sem o consentimento do titular, aliás, coaduna-se com a forma pela qual o sistema “Porta Digitais” foi concebido para coletar imagens de modo dissimulado. Assim se conclui pela camuflagem da câmera no painel eletrônico publicitário em posição tal que passa despercebido ao usuário, atraído para olhar as mensagens publicitárias, ser ele próprio objeto de filmagem não autorizada”.

⁷ Ação Civil Pública nº 1090663-42.2018.8.26.0100; TJSP, consulta realizada no site <http://www.tjsp.jus.br>, acessado em 12/12/2022.

⁸ Parecer do Ministério Público nos autos da Ação Civil Pública nº 1090663-42.2018.8.26.0100 - TJSP

O INDEC apresentou laudos que afirmando que a coleta de dados pessoais mesmo que por um pequeno período são inseridos no sistema o que possibilitaria a aplicação de uma engenharia reversa que traria a identificação do usuário, de forma mais ampla inclusive, com identificação dos chamados metadados, que possibilitam além da identificação obter informações como geolocalização, horário dentre outros.

Por outro lado, parecer trazido pela concessionária afirma que não há um reconhecimento facial do indivíduo e sim, e tão somente, a detecção facial, que consiste em detecção de pontos faciais convertidos em uma sequência numérica que são assim armazenadas e por isso incapazes de identificar e individualizar a pessoa. Esses dados armazenados, serviriam para estatística, informação do usuário do transporte coletivo e com finalidade de melhoria de serviços, reafirmando a impossibilidade de identificação pessoal do indivíduo:

“Durante o transcorrer de todo o processo, os pontos capturados dos rostos humanos e as imagens recebidas da câmera não são armazenados em nenhum tipo de arquivo ou mídia, sendo descartados pelo sistema. O servidor portanto contém armazenado apenas as totalizações dos dados contidos na matriz numérica enviado pelo programa *MATRIX*”⁹.

Dessa forma, defende que há sempre uma anonimização dos dados o que então não infringe quaisquer regras previstas na legislação, vez que não considerados dados pessoais.

Essa demanda foi julgada em abril de 2021 pela 37ª Vara Cível do Foro Central de São Paulo, onde houve a condenação da concessionária ViaQuatro a pagar a indenização no montante de R\$ 100 mil a título de danos morais coletivos, entretanto, referida decisão ainda não transitou em julgado, podendo, portanto, ser revista a nível de recurso.

Da análise do acima exposto, constata-se a importância de uma legislação que estabeleça os limites, o uso e tratamento dos dados obtidos através do reconhecimento facial. A proposta legislativa ora em análise visa estabelecer alguns limites e direitos aos cidadãos, conforme se vê pela leitura do artigo 8º do referido Projeto de Lei¹⁰:

⁹ Laudo pericial apresentado pela ViaQuatro e juntado aos autos da Ação Civil Pública nº 1090663-42.2018.8.26.0100 – TJSP acessado em 12/12/2022

¹⁰ Projeto de Lei nº 4.612/2019.

“Art. 8º. São garantias dos cidadãos afetados pelo desenvolvimento, aplicação e uso das tecnologias de que trata esta Lei, sem prejuízo de outras previstas em legislação:

- I. informações claras e completas sobre o uso de seus dados pessoais para quaisquer atividades componentes das tecnologias de que trata o caput;
- II. respeito à privacidade, à autodeterminação informativa e à liberdade de expressão, de informação, de comunicação e de opinião;
- III. inviolabilidade da intimidade, da honra e da imagem;
- IV. defesa do consumidor, dos direitos humanos, do livre desenvolvimento da personalidade, da dignidade e do exercício da cidadania; e
- V. proibição de instrumentos, políticas e normas de contínua vigilância massiva.”

Observa-se que essa lei visa estabelecer parâmetros de utilização do reconhecimento facial algumas utilizações e segmentos, não tratando de forma aprofundada no que concerne a sua aplicação e utilização para fins de Segurança Pública, determina que cabe à Autoridade Nacional de Proteção de Dados o encargo de colaborar para a criação de uma legislação específica, conforme preceitua o artigo 4º, inciso II do referido Projeto.¹¹

Cria ainda, o Banco Nacional de Reconhecimento Facial e Emocional integrante do Ministério da Justiça e Segurança Pública, que segundo o artigo 12, que trará nova redação ao artigo 7º-D da Lei nº 12.037/2009, ao dispor que:

“Art. 7º - D. Fica autorizada a criação, no Ministério da Justiça e Segurança Pública, do Banco Nacional de Reconhecimento Facial e Emocional que disporá de dados de identificação biométrica facial e emocional das pessoas com mandados de prisão já cumpridos ou não.
§1º. O Banco Nacional de Reconhecimento Facial e Emocional visa subsidiar investigações criminais federais, estaduais ou distritais, e auxiliar na captura de foragidos da justiça”.

Depreende-se da leitura desse artigo que haverá a possibilidade de identificação facial de pessoas a fim de que se busque suspeitos de crimes ou foragidos da justiça. A questão que se segue, surge em relação a segurança dos algoritmos e, portanto, da correta aplicação e abordagem daqueles que por ventura

¹¹ Art. 4º. À Autoridade Nacional de Proteção de Dados (ANPD), criada pela Lei nº 13.853, de 8 de julho de 2019 compete:

.....
II . colaborar com outros setores do Poder Público em todas as esferas, por meio de convênios, visando a elaboração de legislação voltada para o uso da tecnologia de que trata o art. 1º nas áreas da saúde, educação, transporte, segurança pública, assistência social, entre outras;

serão identificados quando da ocorrência de um reconhecimento através dessa tecnologia.

Como já vimos, essa tecnologia apresenta grandes valhas, em razão do viés a que estão submetidas, razão pela qual são vistas como ressalvas em vários países do mundo.

2.4 Projeto de lei nº 1.515/22

Este projeto, do deputado Coronel Armando (PL-SC), dispõe sobre a aplicação da Lei Geral de Proteção de Dados Pessoais (LGPD) para fins de segurança do Estado, de defesa nacional, de segurança pública e de investigação e repressão de infrações penais.

O objetivo deste projeto de lei é justamente regular as permissões do Estado em relação ao acesso, utilização e tratamento de dados pessoais observando as garantias de cada indivíduo disposto no art. 4^a, inciso III da LGPD.

A princípio o projeto traz uma segurança jurídica maior porque regula tema ainda não regulamentado bem como apresenta consonância com os objetivos, princípios e fundamentos da LGPD trazendo um grande avanço quando prevê a responsabilização dos agentes públicos e a proibição de decisões automatizadas.

No entanto, apesar de trazer uma segurança jurídica maior e estar de acordo com a LGPD, o projeto de lei contradiz o princípio da transparência, pois dificulta o acesso aos dados pelo seu titular, podendo haver recusas e demora no fornecimento destas informações.

Não bastasse a dificuldade criada ao acesso aos dados, o PL não menciona a possibilidade do titular dos dados de acompanhar o tratamento dos dados, mas apenas fazer a checagem dos seus dados afrontando princípio do livre acesso aos dados, estabelecidos pela LGPD.

Ainda, outros pontos negativos se sobressaem, em especial em relação ao compartilhamento destes dados com entidades da administração pública e com organização internacional ou agente no exterior que atue na área de segurança

pública, defesa nacional e persecução penal. Podendo até, dependendo do caso, ser compartilhado com pessoas jurídicas de direito privado

O compartilhamento com outros órgãos propicia uma maior possibilidade e probabilidade de vazamento destes dados facilitando a sua exposição e invasão destes sistemas sem que haja proteção suficiente.

O projeto de lei ainda, prevê sanções para o caso de infrações. No entanto as penalidades são tão brandas que o cuidado com estes dados pode não ser tão rigoroso como deveria ser aumentando, portanto, a insegurança da utilização destes dados pelo poder público.

3. ABORDAGEM INTERNACIONAL SOBRE O RECONHECIMENTO FACIAL E SEUS VIESES

Em estudo realizado no 2020¹² constatou que existem cercas de 109 países no mundo que usam ou aprovam a tecnologia de reconhecimento biométrico facial para fins de vigilância. Temos apenas um país que declarou de forma explícita a ilegalidade do uso dessa tecnologia, a Bélgica. Vejamos um apanhado geral do uso dessa tecnologia pelo mundo.

3.1 Europa

Primeiro é importante destacar que a proteção de dados faz parte da Carta de Direitos Fundamentais da União Europeia¹³, que em seu artigo 8º, dispõe:

“Artigo 8º. Proteção de dados pessoais.

1. Todas as pessoas têm o direito à proteção de dados de caráter pessoal que lhes digam respeito.
2. Esses dados devem ser objeto de um tratamento leal, para fins específicos e com o consentimento da pessoa interessada ou com outro fundamento legítimo previsto por lei. Todas as pessoas tem o direito de aceder aos dados coligidos que lhes digam respeito e de obter a respectiva retificação.
3. O cumprimento destas regras fica sujeito a fiscalização por parte uma autoridade independente.”

¹² Estudo elaborado pela Surfshak, uma empresa de tecnologia, instalada nas Ilhas Virgens Britânicas, que oferece basicamente serviços de segurança da informação. Matéria extraída do site: <https://surfshark.com/facial-recognition-map>, acessado em 12/12/2022.

¹³ <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:12012P/TXT> acessado em 12/12/2022

Na prática o uso dessa tecnologia é amplamente difundido na Europa, existem câmeras instaladas em 32 países. Entretanto, esse uso vem sofrendo interferências e sendo objeto de constante ataque de grupos de defesa dos direitos civis.

Em 21 abril de 2021 a Comissão Europeia propôs a utilização dessa tecnologia para fins de localização de crianças desaparecidas, busca de criminosos e possível envolvidos em ataques terroristas. Dois dias, após a Autoridade Europeia de Proteção de Dados¹⁴, que é a agência responsável pela vigilância de privacidade na União Europeia, emitiu um parecer que defende o banimento do reconhecimento facial, alegando em suma, a violação de direitos fundamentais. Declarou a agência, dentre outras questões abordadas, que:

“Uma abordagem mais rígida é necessária, já que a identificação biométrica remota, em que a IA pode contribuir para avanços sem precedentes, apresenta riscos extremamente altos de intrusão profunda e não democrática na vida privada dos indivíduos.”

Constata-se, portanto, o uso com mais cautela dessa tecnologia, bem como a tentativa de elaboração de uma legislação apta a estabelecer limites e garantias de caráter de proteção a privacidade, bem como frear eventuais avanços de viés autoritário por parte dos governantes.

3.2 Estados Unidos

A tecnologia de reconhecimento facial é amplamente utilizada nos Estados Unidos quando a questão é segurança pública, o emprego dessa tecnologia se intensificou após os atentados ocorrido em 11 de setembro de 2001.

Entretanto são vários os relatos prisões ilegais ocorridas em razão da falha do equipamento.

A primeira falha na identificação de uma pessoa com a utilização da tecnologia de reconhecimento facial relatada no país foi na cidade de Detroit, no ano de 2020, esse erro resultou na prisão de um homem negro que foi acusado de roubo de uma loja de roupa de luxo.

¹⁴ https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_pt#documents acessado em 12/12/2022

O homem é Robert Willians, ele foi acusado de no mês de outubro de 2018, ter roubado cinco relógios avaliados em U\$ 3.800,00 e foi preso em sua casa sem qualquer explicação.

Para chegar a identidade de Robert Willians a polícia utilizou a tecnologia de reconhecimento facial, cruzando a imagem feita no local do roubo com o banco de dados onde estão depositadas as imagens de carteira de motoristas dos cidadãos em solo americano.

Essa tecnologia identificou de forma errônea tratarem-se da mesma pessoa. Robert passou uma noite na prisão e foi liberado após o policial dizer que a máquina “deve ter entendido errado”.

Após protestos de entidades e organizações, cinco Estados do país já recuaram em relação ao uso dessa tecnologia, são eles Virginia, Portland, San Francisco, Oakland e Boston.

As gigantes da tecnologia, Microsoft, Amazon e IBM suspenderam a venda de equipamentos de reconhecimento facial para o governo até que as regras para sua utilização sejam melhor delimitadas pelo Congresso Americano.

3.3 China

As câmeras de reconhecimento facial estão espalhadas por todo o país, fazendo com que seja o local mais vigiado do planeta, com suas mais de 200 milhões de câmeras de reconhecimento facial.

Estima-se que o país detenha um banco de dados com aproximadamente 1 bilhão de imagens de cidadãos, o maior banco de imagens do mundo.

Ocorre que pelo próprio sistema de governo aplicado no país, o uso dessa tecnologia não incomoda ou pelo menos já não mais incomoda os cidadãos daquela localidade.

Atualmente as câmeras estão por todas as partes, ruas, shoppings, estádios, teatros, enfim, as câmeras fazem parte da rotina dos chineses, tanto no que concerne a vigilância quanto ao que se refere as prestações de serviços.

Lá é possível entrar em um transporte público sem que se tenha que pagar, a simples autenticação da face já gera o direito ao ingresso.

A pandemia do COVID veio a “agravar” ainda mais essa situação, atualmente em qualquer local que se vá existem câmeras que monitoram o trajeto e sem momento futuro houver a informação de que a pessoa foi contaminada pelo vírus, todas as outras pessoas que estiveram na mesma localidade que o indivíduo infectado são imediatamente avisados a ficarem atentos a quaisquer sintomas e são nomeados como pessoas com potencial de transmissibilidade do vírus, ficando impossibilitada de frequentar certos locais.

Todo esse controle ocorre sem que haja qualquer iniciativa do cidadão que circula pelo país, as câmeras de reconhecimento facial fazem todo o trabalho e permanecem monitorando as pessoas.

Não é exagero afirmar que naquele país o reconhecimento facial funciona como um sistema de vigilância permanente sobre os seus habitantes.

O governo chinês não disponibiliza as informações sobre os dados capturados e tão pouco prevê a anuência quanto a identificação biométrica facial.

4. CONCLUSÃO

Para que o reconhecimento biométrico facial para fins de vigilância ocorra é necessária uma prévia captura dos dados sensíveis dos indivíduos com a finalidade de formação de um banco de dados.

Essa captura na grande maioria das vezes é feita sem a autorização pessoal e ainda sem que haja a informação a seus titulares sobre o destino a ser dado a esses dados pessoais. Tal procedimento fere o disposto na constituição federal, vez que há uma mitigação dos direitos fundamentais da pessoa humana.

Além dos questionamentos relativos à proteção dos dados, em especial os dados sensíveis, a sua utilização pode apresentar vieses capazes de trazer resultados dotados de preconceitos, pois a alimentação dos dados pelos sistemas ainda é feita de forma obscura e utilizado para o aprendizado da máquina.

Há vários sistemas que vem sendo utilizados no mundo pelo poder público que se mostraram eficientes para o fim proposto, entretanto há relatos de equívocos em razão dos vieses inseridos nos algoritmos utilizados pela tecnologia.

Outra questão é a falta de transparência em relação a destinação e o compartilhamento desses dados sensíveis, não se sabe quais são as organizações ou

órgãos governamentais que tem acesso a essas informações e quem seria o responsável por seu armazenamento.

O Brasil ainda avança em termos de legislação específica sobre biometria facial com projetos de lei em tramitação, entretanto, é de se salientar que, até o momento nenhum dos projetos propostos apresentam uma solução satisfatória a fim de garantir os direitos fundamentais resguardados por nossa Constituição Federal.

Assim, a utilização dos dados sensíveis de cada cidadão com ou sem a sua permissão pelo poder público deve ser vista e tratada com muita cautela, pois ainda que o interesse público deva prevalecer sobre o interesse individual, as pessoas não podem ser expostas de forma irresponsável pelo Estado, sob pena de sofrerem mitigação de seus direitos fundamentais e sujeitas a ocorrência de sérios danos por vezes irreparáveis.

REFERÊNCIAS

_____ *The Facial Recognition World Map*. Holanda, 2020. Disponível em <<https://surfshark.com/facial-recognition-map>>. Acesso em: 20 de dezembro de 2022.

AZEVEDO, Cynthia Picolo Gonzaga de; LIMA, Eliz Marina Bariviera de; SILVA, Felipe Rocha da; RODRIGUES, Gustavo Ramos; DUTRA, Luiza Corrêa de Magalhães; SANTARÉM, Paulo Rená da Silva; VIEIRA, Victor Barbieri Rodrigues. **Nota técnica: análise comparativa entre o anteprojeto de LGPD penal e o PL 1515/2022. Instituto de Referência em Internet e Sociedade (IRIS) e Laboratório de Políticas Públicas e Internet (LAPIN), novembro de 2022.** Disponível em: <<https://irisbh.com.br/wp-content/uploads/2022/11/Nota-tecnica-Analise-comparativa-entre-o-anteprojeto-de-LGPD-Penal-e-o-PL-1515-2022.pdf> >. Acesso em: 20 de dezembro de 2022.

BRASIL, Emanuelle. **Câmara dos Deputados**. Agência Câmara de Notícias <<https://www.camara.leg.br/noticias/893704-projeto-altera-lei-de-protecao-de-dados-para-resguardar-seguranca-publica-e-defesa-nacional/>> Acesso em: 12 de dezembro de 2022

BRASIL. Constituição (1988). **Constituição da República Federativa do Brasil**. Brasília, DF: Senado Federal: Centro Gráfico, 1988. Disponível em <http://www.planalto.gov.br/ccivil_03/constituicao/emendas/emc/emc115.htm> Acesso em: 12 de dezembro de 2022

BRASIL. LEI Nº 13.709, DE 14 DE AGOSTO DE 2018. **Lei Geral de Proteção de Dados Pessoais (LGPD)**. Brasília, Diário Oficial da União, 14 de agosto de 2018.

Disponível em <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/113709.htm> Acesso em 03 de dezembro de 2022

FELDSTEIN, Steven. *The Global Expansion of AI Surveillance*. 2019 Carnegie Endowment for International Peace. Disponível em <https://carnegieendowment.org/files/WP-Feldstein-AISurveillance_final.pdf>. Acesso em: 20 de dezembro de 2022.