Revista Brasileira de Direito e Gestão Pública
www.gvaa.com.br/revista/index.php/RDGP/
ISSN: 2358-2405

Reconhecimento facial: análise a partir da Constituição brasileira e da Lei Geral de Proteção de Dados

Facial Recongnition: analysis by brazilian Constitution and General Data Protection Law

Rodrigo Natálicio dos Santos[1], Cristiane Helena de Paula Lima Cabral[2]

v. 8/ n. 5 (2020)
Novembro

Aceito para publicação em 05/09/2020.

[1]Bacharel em Direito pelas Faculdades Kennedy. E-mail: rodrigonatalicio@gmail.com;

[2]Doutora em Direito Público Internacional pela Pontifícia Universidade Católica de Minas Gerais; Mestra em Ciências Jurídico-Internacionais pela Faculdade de Direito da Universidade de Lisboa; Professora Universitária. E-mail: crishelenalima@gmail.com.

https://www.gvaa.com.br/revista/index.php/RDG

Resumo

Este artigo tem por objetivo analisar os riscos inerentes da utilização do reconhecimento facial pelos órgãos estatais e privados, como forma de identificação do indivíduo. Demonstrando que a coleta excessiva de dados, a serem armazenados em sistemas públicos e privados, podem comprometer significativamente a vida dos cidadãos, representando, portanto, em ofensa ao dispositivo Constitucional. Em uma análise jurídico acadêmica da questão, pode-se notar que esta deve submeter-se a uma reflexão pautada no texto Constitucional, considerando os direitos à privacidade e a liberdade do cidadão. Dessa forma, o artigo terá como finalidade a pesquisa aplicada visto se tratar de um aspecto de natureza teórica. Cabe, ainda, destacar que o objetivo teórico-metodológico é exploratório, isto porque, o assunto representa extrema relevância social, pois atinge sobremaneira princípios elencados pela Constituição da República Federativa do Brasil de 1988. Esse artigo se pautará na análise de dados por intermédio da pesquisa de fontes, através da Constituição da República/1988, leis correlatas, bibliografias e artigos científicos. Serão analisados principalmente os fatores que demonstram a inviabilidade do sistema de reconhecimento facial para à sociedade.

Palavras-chave: reconhecimento facial, privacidade, proteção do cidadão.

Abstract

The main purpose of this article is to analyze the risks inherent in the use of facial recognition by state and private bodies, as a way of identifying the individual. Demonstrating that the excessive collection of data, to be stored in public and private systems, can significantly compromise the lives of citizens, representing, therefore, in offense to the Constitutional provision. In an academic legal analysis of the issue, it can be noted that it must undergo a reflection based on the Constitutional text, considering the rights to privacy and freedom of the citizen. Thus, the article will have the purpose of applied research since it is an aspect of a theoretical nature. It is also worth noting that the theoretical-methodological objective is exploratory, because the subject represents extreme social relevance, as it greatly affects principles listed by the Constitution of the Federative Republic of Brazil of 1988. This article will be based on data analysis through the research of sources, through the Constitution of the Republic / 1988, related laws, bibliographies and scientific articles. The factors that demonstrate the unfeasibility of the facial recognition system to society will be analyzed.

Keywords: facial recognition, privacy, citizen protection.

1. Introdução

Ao longo dos anos, os seres humanos vêm buscando a criação e o aprimoramento de ferramentas tecnológicas, com o intuito de propiciar maior comodidade e segurança, quer seja como forma de reduzir e prevenir a violência no seio da sociedade, quer seja para trazer maior segurança no ambiente virtual.

Os constantes avanços tecnológicos, culminaram na utilização de diferentes dispositivos, tanto pelos órgãos públicos, quanto pelos órgãos privados. É fato que algumas dessas tecnologias foram e ainda são bastante eficazes, outras, entretanto, representam riscos à liberdade e à intimidade do indivíduo. Uma espécie de aparato que representa um grande risco para o cidadão, trata-se do mecanismo tecnológico atualmente apresentado como solução para redução dos mais diversos crimes e como instrumento gerador de maior segurança no campo virtual, qual seja, a tecnologia denominada de reconhecimento facial.

Insta salientar que o referido recurso tecnológico tem dividido opiniões, pois representa um alto controle na vida do cidadão por parte do Estado e da iniciativa privada. Além do alto poder de controle, o fator mais preocupante remete-se as falhas apresentadas pela referida tecnologia, que poderá ocasionar em danos irreparáveis na vida do indivíduo, há depender do tipo de exposição e finalidade da utilização dos dados armazenados pelos gestores tecnológicos.

Alguns especialistas têm demonstrado bastante preocupação com o rumo que tomado na utilização do reconhecimento facial, haja vista, que além das violações aos dispositivos legais, a referida tecnologia, opera através de algoritmos de identificação, que por sua vez tem apresentado erros significativos, podendo ocasionar em um aprisionamento de pessoas inocentes e ainda servir como mecanismo de discriminação e controle social. O planejamento de um algoritmo para simulação de uma atividade humana compreende na tentativa de simular o raciocínio, a forma de pensar e realizar tarefas pelo cérebro humano. Porém, vale ressaltar que tal simulação encontra-se completamente distante da complexidade apresentada por nossos cérebros, no que tange ao reconhecimento da face.

A coleta e o armazenamento de dados, que serão utilizados para subsidiar os sistemas de reconhecimento facial ou qualquer outro meio tecnológico que tenha por causa precípua a identificação do indivíduo, são passíveis de manipulação, pois armazenados em bancos de dados dos quais o cidadão não tem acesso, essas informações podem ser manipuladas pelo Governo do

país onde a tecnologia é utilizada, por outros Governos e até mesmo por terceiros com grande poder econômico e tecnológico.

A Constituição da República Federativa do Brasil de 1988, em seu artigo 5º, inciso LVIII, garante ao civilmente identificado o direito fundamental de não ser submetido à identificação criminal, ressalvadas as pouquíssimas exceções previstas na Lei nº 12.037/2009. Desta forma, a apresentação de documento de identificação oficial válido, desobriga o civilmente identificado a registrar seus dados biométricos, sejam eles datiloscópicos ou faciais, compreendendo entre eles os registros fotográficos ou de vídeos.

Levando em consideração que nenhum banco de dados pode reconhecer por si só um indivíduo, mas para que isso ocorra, a sua privacidade, liberdade e intimidade serão violadas, sob o pretexto de que tal violação trará maior segurança. Diante de tal cenário, o desfecho pode ser trágico, vexatório e até mesmo incorrigível, seja em decorrência de suas falhas algorítmicas, seja em decorrência da violação aos direitos fundamentais dispostos na Constituição da República Federativa do Brasil de 1988.

Assim, a pesquisa terá como finalidade a forma aplicada visto se tratar de um aspecto de natureza teórica. Cabe, ainda, destacar que o objetivo teórico-metodológico é exploratório, isto porque, o assunto representa extrema relevância social, pois atinge sobremaneira princípios elencados pela Constituição da República Federativa do Brasil de 1988

2. Metodologia

Para o presente artigo usou-se da análise da bibliografia sobre assunto, incluindo-se diversos artigos que foram apresentandos sobre o tema.

Nesse sentido, optou-se por um objetivo teórico-metodológico de forma exploratória tendo em vista a relevância do tema e os deslindes para a questão da privacidade e dos direitos elencados na Constituição da República Federativa do Brasil.

3. Resultados e Discussão

O reconhecimento facial é uma espécie biométrica de identificação por meio da face, que tem por procedimento a localização automática de rostos, medindo o grau de similaridade entre as duas imagens faciais, com o propósito de identificação do indivíduo ou a sua identidade (OLIVEIRA, 2019).

O sistema de reconhecimento facial divide-se em três etapas, quais sejam, detecção da face, extração de características e reconhecimento da face. No tocante a detecção da face, essa lhe é informada em uma determinada posição e associado a um tamanho e uma orientação, ou seja, no processo de identificação o sistema tem por objetivo determinar a identidade de uma imagem facial desconhecida, tendo por base comparativa diferentes imagens faciais armazenadas em bancos de dados, apresentando um grau de similaridade a cada comparação (BRAGA, 2013).

Desta forma, associa-se, portanto, aquela identidade que alcança o maior grau de similaridade na comparação, via de regra os algoritmos de detecção facial são baseados em detectar o formato do rosto, além de extrair as informações do mesmo como olhos, nariz, boca entre outros.

Após a detecção, ocorre a separação da área de interesse, que nesse caso é a face, desta forma descarta-se o restante da imagem, partindo-se para extração de características, tem como base principal a localização de regiões da imagem que contenham características significativamente relevantes, podendo ser distinguidas por sua textura, forma, intensidade entre outras.

A última etapa do processo refere-se ao reconhecimento da face que consiste em encontrar em meio a um grupo predefinidos de faces aquela que mais se aproxima da face analisada, tendo por base as características extraídas nos processos anteriores.

A utilização da tecnologia de reconhecimento facial ganhou grande relevância no Brasil e no mundo. “Tal processo teve uma grande aceleração em decorrência da criação de aplicações variadas para o recurso. Além da diversificação, o avanço nas técnicas de inteligência artificial tem aumentado a precisão tanto da capacidade de reconhecimento de pessoas quanto do mapeamento de diferentes expressões” (VALENTE, 2018).

Na China, 200 milhões de câmeras compõem um sistema de vigilância capaz de identificar basicamente qualquer um dos 1.4 bilhão de habitantes do país. Na capital dos Emirados Árabes Unidos, Dubai, um gigantesco aquário localizado no principal aeroporto da cidade conta com mais de 80 câmeras de segurança, que escaneiam e analisam o rosto das pessoas à medida que caminham por ele, por fim, o sistema ou permite que a pessoa ingresse livremente no país, ou emite um alerta de segurança. Nos EUA, no ano de 2016, ao menos 50% dos cidadãos adultos já constavam em bases de dados de reconhecimento facial do governo (OLIVEIRA, 2019).

No Brasil o mecanismo de reconhecimento facial, tem sido utilizada por empresas privadas e órgãos governamentais, sob o argumento de gerar maior segurança para a sociedade.

Na atualidade, o direito à intimidade e à privacidade ocupam lugar de destaque nos debates jurídicos, positivando-se em nível constitucional e infraconstitucional na maioria dos países tidos

como juridicamente desenvolvidos. No âmbito internacional ocorre o mesmo fenômeno, pois sendo diversos os tratados, acordos e convenções que versam sobre a sua tutela. Entretanto, faz-se sobremaneira interessante saber a partir de quando os institutos da intimidade e vida privada tornaram-se devidamente protegidos, haja vista as evoluções mundiais do Direito, levando-se em consideração o contexto social.

Nas palavras de André Ramos Tavares (2012), no que tange ao direito à privacidade, seria de competência de seu titular escolher se deve divulgar ou não seus conjuntos de dados, informações, manifestações e referências individuais, e, no caso de divulgação poder decidir quando, como, onde e a quem divulgar. Tais elementos são aqueles que decorrem da vida familiar, doméstica ou particular do indivíduo, e, envolvem fatos, atos, hábitos, pensamentos, segredos, atitudes e projetos da vida. No tocante à intimidade o autor definiu que essa seria a camada ou esfera mais reservada, cujo acesso é de vedação total ou muito restrito, geralmente para familiares. Já a vida privada estará representada por uma camada protetiva menor, embora existente. Muitos podem ter acesso, mas isso não significa a possibilidade de divulgação irrestrita, massiva, ou a desnecessidade de autorização.

No que tange a positivação específica do direito à intimidade e à vida privada em âmbito internacional, MERTENS (2006), descreve que esses decorreram da elaboração da Declaração Americana dos Direitos e Deveres do Homem, de 02 de maio de 1948 e que posteriormente a sua elaboração, mais precisamente em 10 de dezembro de 1948, ocorre a aprovação da Declaração Universal dos Direitos Humanos, pela Assembleia Geral das Nações Unidas (ONU). Dois anos mais tarde, foi editada a Convenção Europeia dos Direitos do Homem, assinada em Roma, quando sedimentou a existência do direito à privacidade.

A Declaração Americana dos Direitos e Deveres do Homem previu em seu art. 5º, que "Toda pessoa tem direito à proteção da lei contra os ataques abusivos à sua honra, à sua reputação e à sua vida privada e familiar". No que concerne à DUDH, está elencado em seu art. 12, que "Ninguém será sujeito à interferência em sua vida privada, em sua família, em seu lar ou em sua correspondência, nem a ataque à sua honra e reputação. Todo ser humano tem direito à proteção da lei contra tais interferências ou ataques".

É importante ressaltar que a positivação do direito à privacidade e à intimidade ocorreu no período pós II Guerra Mundial, período marcado por inúmeros traumas decorrentes da barbárie humana, principalmente na Europa, em decorrência das invasões e arbítrios ocorridos durante a

Grande Guerra. Desde então o direito fundamental da inviolabilidade à intimidade e à vida privada vem se consolidando, tornando-se objeto de constantes debates no âmbito jurídico mundial.

No Brasil o direito à intimidade e à vida privada foram consagrados na Constituição Federal de 05 de outubro de 1988, em seu art. 5º, X. Desta forma constitucionalmente passam a ser tutelados pela Carta Magna ambos os direitos de personalidade, haja vista, não existir previsão de proteção destes atributos da personalidade humana nas constituições anteriores.

Nas palavras de Walber de Moura Agra (2018), os referidos direitos não existiam expressamente na Carta Magna anterior, entrando, portanto, no resguardo constitucional em decorrência da inovação tecnológica. Desta forma, trata-se de garantias, para a proteção dos cidadãos contra os avanços tecnológicos que possuem por finalidade devassar a vida das pessoas. Entretanto, nota-se que na França, já no século passado, a preocupação em virtude da divulgação de fotos de pessoas célebres da época já era manifestamente existente.

Ademais, o artigo 5º da CRFB/1988, em seu inciso XI, descreve a casa como asilo inviolável do indivíduo, local este, próprio para se desenvolver grande parte das condutas intimas e privadas. No inciso XII, do mesmo artigo, menciona-se a proteção ao sigilo das comunicações telegráficas, de dados e telefônicas, que conforme se pode notar, fazem parte dos direitos à vida privada. Portanto, pode-se perceber que o legislador buscou resguardar sobremaneira esses atributos de personalidade, demonstrando total preocupação, assegurando que fossem devidamente protegidos de qualquer tipo de violação.

Com o avanço significativo da tecnologia e das relações humanas, é de suma importância que se busquem formas de coibir eventuais excessos por parte dos órgãos estatais e privados, no que tange a manipulação de dados. Tantas inovações tecnológicas, tem de certa forma desnudado a intimidade e privacidade das pessoas, sem que em alguns casos se deem conta dos riscos inerentes de tal exposição.

Em grande parte dos países ao redor do mundo, o fortalecimento das práticas de segurança e privacidade de dados, culminaram em diversas regulamentações, que buscam como aspecto principal a proteção do indivíduo. A preocupação por parte dos órgãos reguladores, quanto por parte das empresas e dos cidadãos, apresenta-se de formato crescente, pois a manipulação de dados de forma indevida pode ocasionar em prejuízos imensuráveis. Desta forma, a implementação de regras específicas sobre o tema torna-se uma questão urgente e fundamental.

Cada país possui suas peculiaridades, mas a proteção à intimidade e à privacidade é uma preocupação mundial. Portanto, a criação de regramentos que protejam os atributos de

personalidade supracitados, baseia-se em outros regramentos que se mostraram eficazes e ou naqueles que sucumbiram por ineficiência. Assim observando os acertos e falhas, cada país busca construir uma base forte que resguarde os direitos de seus cidadãos.

1. Legislação brasileira

Diante do grande avanço tecnológico e da necessidade constante de alterações para maior adequação, foi editada a Lei 13.709 de 14 de agosto de 2018, Lei Geral de Proteção de Dados (LGPD), estabeleceu-se como medida reguladora do tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado.

O legislador buscou proteger sobremaneira o cidadão de eventuais excessos praticados pelos órgãos públicos e privados. Vale ainda destacar que a privacidade é a primeira a ser disposta no referido artigo, haja vista sua relevante importância no que tange a personalidade do indivíduo.

Com o advento das inovações tecnológicas que propiciaram um maior fluxo de dados, surge a necessidade de uma nova lei que trouxesse maior segurança jurídica, padronizando normas e práticas, promovendo, portanto, a proteção aos dados pessoais de todo cidadão de forma igualitária, dentro do país e no mundo. A lei apresenta imediatamente em seu início de forma que não haja dúvida, o que são dados pessoais, definindo ainda em alguns casos um tratamento mais específico à determinadas informações, como é o caso dos dados sensíveis e os sobre crianças e adolescentes, tratados tanto no meio físico como nos digitais estão sujeitos a regulação.

A Lei Geral de Proteção de Dados descreve ainda ser indiferente a localização da sede de uma organização ou o centro de dados, ou seja, não importa se localizados no Brasil ou no exterior, existindo processamento de dados de brasileiros ou não, que estão no território nacional, a lei deve ser cumprida. Não obstante, determina ainda, que é permitido compartilhar dados com organismos internacionais e com outros países, desde que existam protocolos seguros ou para cumprimento de exigências legais.

Antes da LGPD, não existia no Brasil uma lei específica, sendo, que desta forma a regulação da matéria, ocorria por intermédio de algumas leis esparsas, como Código de Defesa do Consumidor (CDC), Lei nº 12.527/2011 - Lei de Acesso à Informação, Lei do Cadastro Positivo – Lei nº 12.414/2011, pelo chamado "Marco Civil da Internet", Lei 12.965/2014 e seu decreto regulamentador nº 8.771/2016, entre outras. Os dispositivos legais descritos estabeleceram

princípios e garantias para o uso da internet no Brasil, apresentando requisitos mínimos para tratamento e gestão de dados.

Mesmo diante de sua total necessidade, haja vista, a quantidade de dados colhidos dia após dia, sem qualquer consentimento, suas penalizações somente terão aplicabilidade a partir de agosto de 2021, ou seja, um ano após o prazo originalmente aprovado. Diante disso, a Lei Geral de Proteção de Dados, agora passará a vigorar somente em 1º de janeiro de 2021. Assim, apesar das sanções estarem com previsão de aplicabilidade a partir de agosto, não haverá óbice em relação ao início de demandas judiciais, que poderão iniciar-se no mês de janeiro de 2021. (DEMARTINI, 2020)

Vale ressaltar, que as datas apresentadas podem sofrer novas alterações conforme entendimento legislativo, o que automaticamente postergaria a entrada em vigor da referida Lei Geral de Proteção de Dados.

Riscos inerentes à utilização do reconhecimento facial

O sistema de reconhecimento facial opera através da submissão de imagens a algoritmos, que possuem como finalidade identificar pontos que são únicos na face de cada indivíduo. O sistema opera através de imagens armazenadas em banco de dados públicos ou privados e busca com velocidade excepcional os pontos faciais de um determinado indivíduo, que teve sua imagem captada por alguma câmera.

No país de Gales, no Reino Unido, a polícia utiliza o reconhecimento facial em grandes eventos, como forma de identificar possíveis criminosos. Durante a final da Champions League, o sistema realizou o registro de 170 mil cidadãos, identificando 2.470 pessoas como criminosos. O problema, no entanto, é que dessas pessoas 2.297, nunca cometeram qualquer tipo de crime. (TECMUNDO, 2018).

Implantado no Brasil por alguns órgãos da segurança pública, o sistema biométrico de reconhecimento facial, vem ganhando espaço significativo, desconsiderando os problemas que a referida tecnologia apresenta, desde falhas em seus algoritmos que comprometem sua eficiência ao acusar falsos positivos na detecção de indivíduos, além de configurar em desrespeito aos dispositivos legais, contrapondo-se a garantia à intimidade e vida privada do indivíduo, previstas na Constituição da República Federativa do Brasil de 1988.

Um exemplo da referida falha algorítmica supracitada, ocorreu na cidade de Copacabana no estado do Rio de Janeiro, onde uma mulher foi identificada através do sistema de reconhecimento facial, que atestou que a identificada tratava-se de uma criminosa foragida da polícia, pela prática dos crimes de homicídio e ocultação de cadáver. Após ser detida e encaminhada à delegacia, a mulher teve sua liberação efetuada aproximadamente uma hora após o ocorrido. Existe ainda um detalhe de extrema relevância a ser considerado, pois a verdadeira criminosa se encontra presa desde o ano de 2015, informação desconhecida pelos policiais militares no momento da prisão. A situação descrita representa, uma clara ofensa à sua dignidade, uma vez, que foi abordada em via pública, presa e conduzida tornando-se notícia em vários veículos de comunicação.

Desta forma pode-se perceber que o Estado não pode buscar a obtenção de resultados colocando em segundo plano a dignidade do indivíduo, ao contrário, ele possui o dever de zelar pela plenitude do princípio elencado na Carta Magna.

Além do exposto, a tecnologia de reconhecimento facial viola outras disposições previstas na Constituição de 1988, como por exemplo, o descrito no artigo 5º, inciso LVIII, que estabelece a não submissão do civilmente identificado à identificação criminal:

Analisando o respectivo dispositivo constitucional, pode-se perceber que a tecnologia denominada reconhecimento facial, bem como, qualquer outra forma de reconhecimento biométrico, contraria o texto constitucional, com algumas ressalvas descritas no § 3º da Lei nº 12.037/2009, que prevê em determinadas situações que até mesmo o civilmente identificado, poderá ser submetido a identificação criminal. Em uma visão garantista, para assegurar que o reconhecimento facial fosse utilizado sem ofensa ao artigo 5º, inciso LVIII, da Constituição da República Federativa do Brasil de 1998, outra norma deveria ser criada regulamentando a utilização da referida tecnologia por parte do Estado.

Mikhail Vieira de Lorenzi Cancelier descreve sobre o direito à privacidade além do âmbito doméstico, da seguinte forma:

> Com o passar do tempo, percebeu-se que mais objetos poderiam repousar sobre sua tutela e que as maneiras de o exercitar não estavam restritas à sua original postura passiva. Intimidade, vida privada, sigilo, dados pessoais, seja qual for o âmbito da expressão humana estudada, entende-se que todos fazem parte da privacidade sendo, cada um ao seu jeito, essenciais à construção da personalidade do indivíduo e, consequentemente, da sociedade como um todo. No atual mundo digitalizado, como já ressaltado, o exercício do direito à privacidade será assegurado mesmo "em público", não sendo mais limitado ao que não é exposto. A privacidade está presente mesmo quando há exposição, mesmo quando há compartilhamento da informação. (CANCELIER, 2017).

Desta forma, resta claro que o Estado, ao valer-se da tecnologia de reconhecimento facial, mesmo que com a premissa de zelar pela segurança, descumpre requisitos legais e viola direitos. A utilização de diferentes tecnologias de reconhecimento tem cerceado o direito dos cidadãos de terem sua privacidade preservada. "De fato, se podemos circular entre os diversos espaços, o fazemos, contudo, sob o olhar atento das câmeras que nos vigiam e nos pedem para sorrir. " (CARVALHO, 2008, p.705).

Em uma análise constitucional da matéria, constata-se que não existe por parte do Estado, o direito de monitorar constantemente os cidadãos, implicando, portanto, tal monitoramento indiscriminado em uma afronta ao dispositivo constitucional. O Estado possui o dever como guardião das Leis de cumpri-las e fazer com que sejam cumpridas, buscando um equilíbrio entre a utilização dos mecanismos para o combate à criminalidade, sem que ocorra qualquer tipo de violação aos direitos e garantias inerentes à pessoa humana.

Ofensa ao direito de privacidade

Apesar de uma parcela da doutrina considerar importante a diferenciação entre os termos privacidade e intimidade, não se enxerga óbices no uso da expressão direito à privacidade como forma de tratar também do direito à intimidade, pois nitidamente um está sobremaneira ligado ao outro. (CANCELIER, 2017).

Conforme já fora descrito, a proteção ao direito à privacidade e à intimidade do cidadão estão elencados no art. 5º, inciso X, da Constituição da República. Tal disposição tem como causa precípua, a limitação do poder do Estado e das empresas privadas, em relação ao monitoramento constante do indivíduo.

O direito à vida privada vem sendo violado constantemente pelos olhares ocultos por detrás das câmeras de vigilância, podendo ser descrito da seguinte forma:

> Atualmente, o direito à vida privada tem sido minado de maneira fulminante com a disseminação da tecnologia, com a instalação de aparelhos registradores de imagens, de dados e até de sons, tanto por parte do setor privado quanto pelo Poder Público. O Estado tem utilizado cada vez mais o controle de imagens para fins de segurança pública. Esse controle, contudo, acaba interferindo na vida privada das pessoas. (TAVARES, 2012, p.689).

Para que o indivíduo conviva em sociedade faz-se necessário estar em meio ao público de uma forma geral, através da utilização de locais comuns de utilização coletiva, quais sejam, praças,

restaurantes, bibliotecas, museus, clubes etc. De uma forma direta, tal utilização ocorre dentro da rotina dos cidadãos. Portanto, a permanência do indivíduo nesses locais não pode ser interpretada como ausência de tutela constitucional. Trata-se da tutela ainda alcançada pela vida privada (e também pela proteção constitucional concedida à imagem). (TAVARES, 2012).

O direito à privacidade não pode ser interpretado de forma restrita, pois se assim o fosse, os indivíduos teriam de viver reclusos em suas casas, não podendo desfrutar de liberdade fora de tal ambiente.

Os métodos de identificações biométricas, da maneira que veem sendo aplicados, ofendem o direito à privacidade tutelado pela Constituição Federal, ao coletarem dados e monitorarem o cidadão de maneira constante e sem o seu consentimento. Desta maneira, sobre a utilização das tecnologias, pode-se dizer que:

> Assim, por evidente que se há de reconhecer que se está a experimentar um gradual esvaziamento da privacidade, especialmente das possibilidades efetivas de sua real proteção, o que não significa que não continuem existindo espaços de maior blindagem e ao menos, ainda que corriqueiras as intervenções na esfera privada, mecanismos de reparação *a posteriori*. (SARLET; MARINONI; MITIDIERO, 2017, p.493).

Todo cidadão mesmo que esteja em locais públicos, possui um certo grau de anonimato, haja vista que grande parte das pessoas que ali se encontram não possuem o menor conhecimento de quem seja aquele determinado indivíduo, desde que é claro, não seja ele uma figura pública. Tal pessoa pode locomover-se no metrô, ônibus e qualquer outro meio de transporte, sem ser reconhecido em nenhum momento. Ocorre, porém, que se uma câmera de segurança realizar o reconhecimento da face o identificando, poderá vincular sua identidade física à sua identidade digital e fazê-lo sem obter seu consentimento primeiro.

Discriminação racial e social

A tecnologia de reconhecimento facial[1] trabalha com algoritmos que necessitam ser treinados, para que dessa forma possa realizar o reconhecimento do indivíduo. Diante dessa

[1] Insta salientar, que a International Business Machines (IBM) abdicou do desenvolvimento e fornecimento da tecnologia de reconhecimento facial, diante do cenário elencado, suas concorrentes nesse ramo tecnológico, quais sejam, Microsoft e Amazon, suspenderam por um ano o uso da referida tecnologia pelas forças policiais, estabelecendo esse prazo para que os governos regulamentem o uso da tecnologia, criando regramento que não permita seu uso como ferramenta discriminatória, perseguições políticas e controle social.

situação existe uma grande preocupação no que tange a precisão da referida tecnologia em grupos étnicos e raciais.

Estudos realizados nos Estados Unidos demonstram que as falhas do sistema de reconhecimento facial atingem afrodescendentes e asiáticos ao acusarem falso positivo nas identificações, além de alguns algoritmos atribuírem sexo errado para mulheres de pele negra.

A Universidade da Califórnia (UCLA) abdicou do uso do reconhecimento facial em seu campus, pois a tecnologia ainda em fase de avaliação, tendo por intuito a identificação de indivíduos frequentadores do local apresentou falhas significativas. Após a realização de testes por intermédio de software foram comparadas 400 faces de integrantes da comunidade universitária (alunos, professores e funcionários) aos rostos de indivíduos criminosos e contraventores devidamente cadastrados, nessa análise ao menos cinquenta e oito falsos positivos, foram computados. Ressalta-se que a maior parte dessas falhas ocorreram na avaliação de rostos de pessoas não brancas.

O teste foi realizado pela ONG Fight For The Future, que procedeu a experiência com um software da Amazon chamado Rekognition. Em um dos casos, a ferramenta atestou em 100% que os rostos, ora comparados seriam da mesma pessoa, mas eram apenas dois homens negros de barba, com traços significativamente diferentes um do outro. (ÉPOCA, 2020)

Vale ressalta que a tecnologia de reconhecimento facial, possui problemas elementares, assim como as demais tecnologias, um dos mais preocupantes refere-se a sua eficácia. Existe por parte dos órgãos estatais e entidades privadas, um certo entusiasmo em referência a esse recurso, desconsiderando, assim, as limitações que ainda marcam seu estágio atual de desenvolvimento. Deve-se destacar que sistemas de reconhecimento facial só apresentam resultados satisfatórios quando as imagens analisadas são fotografias frontais com boa iluminação e resolução. (RODRIGUES, 2019).

Um fator preocupante, além da coleta excessiva de dados por empresas privadas, seria o monitoramento constante por parte do Estado, haja vista o grande acervo de fotos armazenados pelo sistema prisional e demais órgãos de segurança. Com uma população carcerária predominantemente negra, que por sua vez advém de aglomerados e regiões mais carentes, seriam esses locais, portanto, em um país que perpetua fortemente o preconceito racial e social, os que sofreriam um monitoramento constante.

Desta forma, sempre que a pauta remete a vigilância no Brasil, devemos atentar que o direcionamento da lente punitiva do Estado, passará pelo escopo do critério racial e social (SILVA, 2019).

4. Considerações Finais

Diante dos apontamentos apresentados, mostra-se nítido, que o reconhecimento facial representa um risco elevado à intimidade e à privacidade do cidadão.

Além do risco à intimidade e à privacidade, tal ferramenta pode servir como meio discriminatório, basta lembra, que possuímos um sistema carcerário de predominância negra, o que já é suficiente para demonstrar a seletividade discriminatória. Podemos dizer, portanto, que são esses indivíduos, os maiores doadores de dados biométricos para treinamento do referido sistema de reconhecimento facial que deverá ser utilizado em nosso país. O fato de possuirmos um sistema prisional seletivo, mostra que os olhares do Estado permanecem fixos nas origens raciais e sociais com uma maior intensidade. Ademais, com a polarização política e o enfraquecimento dos poderes ao longo dos anos, permitindo ataques vedados pela Constituição da República, torna-se eminente o risco de ocorrerem perseguições políticas contra indivíduos que se oponham a um determinado regime político.

Certo é que os órgãos estatais não têm segundo a CRFB/88, o direito de monitorarem o cidadão de forma constante, devassando sua vida e em determinados momentos causando-lhe constrangimentos, que dependendo das circunstâncias, podem ser irreparáveis. No entanto, vale ressaltar que tal vedação ao monitoramento indiscriminado não se estende somente ao Estado, mas também as empresas privadas, que por sua vez devem zelar pela segurança dos dados coletados independentemente de qual seja. Por isso, a importância da Lei Geral de Proteção de Dados Pessoais - LGPD, que vem sofrendo constante postergação, deixando definitivamente ainda mais vulnerável os direitos do cidadão, que por sua vez é a figura mais frágil nessa relação, frente a descontrolada coleta de dados pessoais.

A tecnologia biométrica denominada de reconhecimento facial possui seu grau de importância, não se pode negar tal fato, até mesmo por tratar-se de ser algo inevitável, em detrimento da evolução humana e automaticamente de suas necessidades. Entretanto, sem os devidos ajustes necessários para seu funcionamento, torna-se totalmente inviável sua utilização. Insta salientar, que os referidos ajustes são de suma importância, mas ainda mais relevante a saber é a conscientização daquele que possui por responsabilidade o gerenciamento e treinamento do

sistema, impedindo, portanto, que a operação se paute em viesses. Assim, deve ser também a orientação, conscientização e treinamento do gerenciador um fator devidamente trabalhado e fiscalizado, seja pelos órgãos públicos ou privados.

Diante de tal circunstância pode-se afirmar que o indivíduo ou órgão responsável pelo gerenciamento, deve possuir acima de tudo preparo técnico e conhecimento das diferenças sociais, que culminam desde os primórdios até os dias atuais em uma acepção grandiosa, penalizando uma grande parcela de desafortunados, que são rotulados pela cor, local em que residem e suas vestimentas, portanto, não se trata de conhecimento social para benefício de determinada classe, mas sim para que possa lidar de forma adequada com a referida tecnologia, mantendo sempre um olhar imparcial, não discriminatório ou político sobre os cidadãos, distanciando o foco de sua câmera da cor, raça, religião, status social ou convicções políticas.

Nesse aspecto, percebe-se a mais lídima necessidade de um dispositivo regulador para proteção de dados dos cidadãos contra abusos cometidos por órgãos estatais ou privados. Portanto, os adiamentos constantes quanto à entrada em vigor da Lei Geral de Proteção de Dados Pessoais - LGPD contribui para perpetuação da vulnerabilidade e coleta de dados de forma indiscriminada, colocando em risco à intimidade e à privacidade dos cidadãos.

Referências

AGRA, Walber de Moura. **Curso de Direito Constitucional.** 9ª ed. Belo Horizonte: Fórum, 2018.

Borelli e Françolin Advogados. **Aplicativo de Reconhecimento Facial fere o direito individual.** Disponível em: https://bfadvogados.wordpress.com/2015/06/21/o-aplicativo-de-reconhecimento-facial-fere-o-direito-individual/. **Acesso em:26 abr. 2020**

BRAGA, Luiz Felipe Zenicola, **Sistema de Reconhecimento Facial,** São Carlos: ANO 2013. Disponível em: http://www.tcc.sc.usp.br/tce/disponiveis/18/180450/tce-08112013-145721/?&lang=br.

BRASIL. **Câmara dos Deputados.** Governo quer lei para regular vigilância estatal por meio de reconhecimento facial. **Disponível em:** https://www.camara.leg.br/noticias/554826-governo-quer-lei-para-regular-vigilancia-estatal-por-meio-de-reconhecimento-facial/. **Acesso em: 26 abr. 2020**

BRASIL. Constituição (1988). Constituição da República Federativa do Brasil. Brasília: Senado Federal, 1988.

BRASIL. Lei 13.709, de 14 de agosto de 2018. **Lei Geral de Proteção de Dados Pessoais**, Brasília, DF, mar 2018.

CANCELIER, Mikhail Vieira de Lorenzi. **O Direito à Privacidade hoje: perspectiva histórica e o cenário brasileiro,** Santa Catarina: ANO 2017. Disponível em: https://www.scielo.br/pdf/seq/n76/2177-7055-seq-76-00213.pdf. **Acesso em: 08 de maio de 2020**

CARVALHO, Kildare Gonçalves. **Direito Constitucional.** 14. ed. Belo Horizonte: Del Rey, 2008.

COSTA, Ramon Silva; OLIVEIRA, Samuel Rodrigues de. **Uso do Reconhecimento Facial em Sistemas de Vigilância e suas Implicações no Direito à Privacidade.** Revista de Direito, Governança e Novas Tecnologias, e-ISSN:2526-0049, Belém, v.5 I, n.2, p.01 – 21, Jul/Dez.2019.

Época Negócios. **Sistema de I.A. falha em identificar pessoas não brancas e universidade desiste de usar reconhecimento facial.** Disponível em: https://epocanegocios.globo.com/Tecnologia/noticia/2020/02/racismo-em-i-leva-universidade-desistir-de-reconhecimento-facial-no-campus.html. **Acesso em 08 de maio de 2020**

KUNDERA, Milan. A imortalidade. 2ª ed. Rio de Janeiro: Nova Fronteira, 1990.

MERTENS, Fábio Alceu, **Análise histórica e legislativa do princípio constitucional da inviolabilidade à vida privada e à intimidade.** Revista Eletrônica Direito e Política, Itajaí, v. 1, n. 1, 3º quadrimestre de 2006. Disponível em: www.univali.br/direitoepolitica.

Minuto da Segurança. **Reconhecimento Facial Ameaça Direitos Básicos de Privacidade.** Disponível em: https://minutodaseguranca.blog.br/reconhecimento-facial-ameaca-direitos-basicos-de-privacidade/. **Acesso em 08 de maio de 2020**

PEZZI, Ana Paula Jacobus, **A Necessidade de Proteção dos Dados Pessoais nos Arquivos de Consumo: em busca da concretização do direito à privacidade.** São Leopoldo: ANO 2007, p.24-25. Disponível em: http://www.dominiopublico.gov.br/download/teste/arqs/cp042824.pdf

RODRIGUES, Gustavo. **Reconhecimento Facial na Segurança Pública: Controvérsias, riscos e regulamentação**. Blog, Instituto de Referência em Internet e Sociedade, 27 de fevereiro de 2019. Disponível em: http://irisbh.com.br/reconhecimento-facial-na-seguranca-publica-controversias-riscos-e-regulamentacao/. Acesso em 15 jun. 2019.

SARLET, Ingo W; MARINONI, Luiz G; MITIDIERO, Daniel. **Curso de Direito Constitucional.** 6 ed. São Paulo: Saraiva, 2017

TAVARES, André Ramos. **Curso de Direito Constitucional.** 10ª ed. São Paulo: Saraiva, 2012.

Tecmundo. **Gales: reconhecimento facial da polícia registra 92% de falso positivo.** Disponível em: https://www.tecmundo.com.br/seguranca/130012-reconhecimento-facial-policia-registra-92-falso-positivo.htm. **Acesso em 08 de maio de 2020**

VALENTE, Jonas. **Tecnologias de Reconhecimento Facial se Popularizam e Levantam Debate.** Agência Brasil. 21 de julho de 2018. Disponível em: https://agenciabrasil.ebc.com.br/geral/noticia/2018-07/tecnologias-de-reconhecimento-facial-se-popularizam-e-levantam-debate Acesso em: 30 de abr. 2020

VIANNA, Túlio Lima. **Transparência pública, opacidade privada: o Direito como instrumento de limitação do poder na sociedade de controle,** Curitiba: ANO 2006. Disponível em: https://acervodigital.ufpr.br/handle/1884/5281