A NECESSÁRIA REGULAÇÃO DO RECONHECIMENTO FACIAL NO BRASIL DIANTE DOS RISCOS À INTIMIDADE E À PRIVACIDADE

Bruno Bastos de Oliveira
Professor do Programa de Pós-graduação em Direito da Universidade de Marília – PPGD UNIMAR. Doutor em Direito pela Universidade Federal da Paraíba – UFPB.
bbastos.adv@gmail.com.

Glesler Sales Maldonado
Auditor-Fiscal da Receita Federal do Brasil. Doutorando no Programa de Pós-graduação em Direito da Universidade de Marília – PPGD UNIMAR.
gleslermaldonado@gmail.com.

RESUMO

O presente trabalho tem como objetivo demonstrar que a ausência de regulação específica no tocante à coleta, ao armazenamento e à destinação de dados biométricos provenientes do uso de tecnologias de reconhecimento facial pode resultar em graves danos a direitos e liberdades constitucionalmente garantidas. Como metodologia de pesquisa utilizou-se do método de abordagem dedutivo e, para análise do tema, foram pesquisadas as bibliografias e o arcabouço normativo e científico concernente ao direito fundamental à privacidade e à intimidade e ao atual estágio de regulação do uso da tecnologia de reconhecimento facial no ordenamento jurídico brasileiro. Conclui-se ser extremamente necessário a regulação do reconhecimento facial no Brasil, sob pena de lesão aos direitos fundamentais, em especial os direitos à privacidade e à intimidade, enfraquecendo os pilares sob os quais repousa o atual Estado Democrático de Direito.

Palavras-chave: Dados biométricos. Intimidade. Privacidade Reconhecimento facial. Regulação.

REGULATION OF FACIAL RECOGNITION IN BRAZIL IN LIGHT OF THE RISKS TO PRIVACY AND INTIMACY

ABSTRACT

The aim of this paper is to demonstrate that the absence of specific regulation regarding the collection, storage, and destination of biometric data from the use of facial recognition technologies can result in serious damages to constitutionally guaranteed rights and freedoms. As a research methodology, the deductive approach method was used and, for the analysis of the theme, the theoretical framework researched the normative and scientific framework concerning the fundamental right to privacy and intimacy and the current stage of regulation of the use of recognition technology in Brazilian legal system. It is concluded that the regulation of facial recognition in Brazil is extremely necessary, under penalty of damage to fundamental rights, in particular the rights to privacy and privacy, weakening the pillars under which the current Democratic Rule of Law rests.

Keywords: Biometric data. Intimacy. Privacy Facial recognition. Regulation.

INTRODUÇÃO

Desde o início de sua vida, o ser humano aprende a identificar o que é um animal, uma árvore, uma cadeira etc. Aprende-se, desta forma, a distinguir itens inanimados, pessoas, animais e sentimentos. Para isto, a mente humana trabalha com memórias das mais variadas fontes e, à medida que a interação social aumenta, redefine-se os limiares do que é conhecido ou não pelo agente. O entendimento e a codificação dessa forma de aprendizagem objetiva o desenvolvimento de técnicas para a definição de modelos para reconhecimento facial.

Através da tecnologia de *machine learning*, os algoritmos automatizam a busca por registros faciais, analisam e desenham relações por meio de diferentes categorias de fisionomias. O *software* ou aplicativo de reconhecimento facial pode valer-se tanto do processo de apresentação estática ou em fluxo, como gravações de imagens em câmeras de um circuito fechado de TV.

Após mais de meio século, desde as primeiras iniciativas, tratando-se do reconhecimento facial automatizado, a sociedade encontra-se em um imbróglio junto a formadores de políticas públicas e à iniciativa privada que, em um campo com incipiente regulação específica a respeito do tema, desenvolve e implementa tal tecnologia sem limites e controles.

Noutra senda, seja pelas denúncias de Edward Snowden em 2013, Cambridge Analytica em 2017, ou ainda diversos eventos de divulgação de dados e utilização inapropriada de informações pessoais, as inovações tecnológicas são cercadas por apreensões concernentes à proteção de dados e ao risco de lesão a direitos fundamentais tais como a privacidade e a intimidade.

Neste sentido, o presente trabalho tem como objetivo demonstrar que a ausência de regulação específica no tocante à coleta, ao armazenamento e à destinação de dados biométricos provenientes do uso de tecnologias de reconhecimento facial pode resultar em graves danos a direitos e liberdades constitucionalmente garantidas, enfraquecendo, deste modo, o atual Estado Democrático de Direito.

Como metodologia de pesquisa utilizou-se do método de abordagem dedutivo e, para análise do tema, foram pesquisadas as bibliografias e o arcabouço normativo e científico concernente

ao direito fundamental à privacidade e à intimidade e ao atual estágio de regulação do uso da tecnologia de reconhecimento facial no ordenamento jurídico brasileiro.

Na primeira seção, fez-se uma análise do direito fundamental à privacidade e à intimidade, demonstrando, sob o prisma constitucional e doutrinário, que a tutela desta esfera pessoal do indivíduo – limitada pela intimidade e privacidade – é imprescindível para resguardar sua realidade enquanto ser humano pleno em dignidade. Na segunda seção, foi analisada especificamente a tecnologia de reconhecimento facial automatizado e sua metodologia de aplicação, composta por três processos distintos: registro, verificação e identificação biométrica. Por fim, na terceira seção, examinou-se o atual estágio regulatório concernente à utilização do reconhecimento facial no Brasil.

1. O DIREITO FUNDAMENTAL À PRIVACIDADE E À INTIMIDADE

Em uma primeira oportunidade, pode-se citar como tutela central ou originária ao direito à privacidade e intimidade, da qual retiram substrato todas as outras espécies de defesa dispostas em leis infraconstitucionais, o artigo 5º, inciso X da Constituição Federal de 1988, que assim dispõe: "são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação" (BRASIL, 2019).

Conforme lembram Eduardo Rocha Dias e Ronald Fontenele Rocha (2019, p. 147):

> [...] no que tange ao catálogo de direitos fundamentais na Constituição brasileira, frise-se que esta albergou, além daqueles direitos nela expressos no título II, também os implícitos e os decorrentes de tratados internacionais de que o Brasil seja parte, bem como outros positivados em toda a Constituição [...]

Ao contrário do que se sucedia em constituições pretéritas, as quais traziam passagens que tinham impacto sobre a privacidade, como por exemplo, a inviolabilidade de domicílio e o sigilo de correspondências e comunicações, entretanto, não faziam uso da terminologia privacidade ou intimidade de maneira expressa, o art. 5º, inciso X, da Lei Maior determina de forma expressa o amparo constitucional sobre a privacidade e intimidade, o que, indiscutivelmente, comprova grande avanço constitucional na defesa a esses importantes direitos (ROSA; FERRARI, 2014).

Destarte, faz-se mister destacar que o direito à intimidade foi elevado ao estado de direito subjetivo constitucional, colocando fim na celeuma referente à presença de um direito geral a intimidade no ordenamento jurídico, que em sede deste preceito constitucional não pode mais ser colocada em xeque. No entanto, um aspecto a ser levado em consideração na busca de se estabelecer a defesa mais efetiva a esses direitos é a situação de que por serem normas de caráter subjetivo (privacidade e intimidade), as fronteiras entre aquilo que pode ou deve ser encarado como público e aquilo que pode ou deve ser reputado como privado possa sofrer variação de indivíduo para indivíduo (SILVA, 2003).

No esforço de encontrar uma tutela que traga efetividade ao amparo do direito fundamental à privacidade e intimidade, é provável se deparar com vários desdobramentos desses direitos em diferentes dispositivos da legislação pátria, como alguns apontando objetivamente para a defesa do direto à privacidade e à intimidade, e outros que resguardam tais direitos sem constar de maneira expressa na norma. Pode-se citar, por exemplo, o amparo trazido pelo artigo 21, do Código Civil, resultado do denominado processo de "Constitucionalização do Direito Privado", o qual determina ser a vida privada do indivíduo inviolável, ficando a cargo do juiz, quando instado pela outra parte, aplicar medidas com o objetivo de obstar ou fazer com que se cesse qualquer prática passível de violar tal norma (FACCHINI NETO, 2003).

O dispositivo mencionado acima carrega para o direito privado o amparo constitucional à intimidade e à privacidade, fazendo com que não paire qualquer tipo de dúvida no tocante a efetividade e vínculo dessa salvaguarda constitucional também na seara do direito privado. Isto é, o mencionado dispositivo fortalece a compreensão de que os direitos fundamentais à privacidade e à intimidade são direitos a serem concretizados de maneira a balizar a atividade do Estado, no entanto, de igual modo dos particulares entre si, com a finalidade de proteger a inviolabilidade de um espectro individual do cidadão demarcado pela intimidade e privacidade.

Nesse sentido, o que se pode deduzir é que ao proteger a seara individual do titular contra interferências do Poder Público e dos outros cidadãos, o direito à privacidade evidencia-se como característico direito de defesa. No entanto, a efetividade do direito à privacidade demanda não somente uma abstenção do poder público, mas igualmente uma atuação do Estado, com o objetivo de assegurar a não ingerência de terceiros na intimidade e na vida privada de outras pessoas, isto é, necessita um desempenho ativo do poder estatal (RUARO, 2013).

Outrossim, a proteção a respeito da privacidade e intimidade espelha-se no sentimento de liberdade da pessoa, sentimento este que indubitavelmente possui estreito relacionamento com a própria dignidade da pessoa humana. Nesta esteira, para ser livre e para – de forma efetiva - poder sê-lo, a pessoa deve ter sua intimidade e sua vida privada resguardadas, sendo detentor de um ambiente pessoal (ou por ventura junto àqueles que lhe são mais próximos), no qual nenhum indivíduo possa adentrar sem sua chancela (KARAM, 2009).

Neste mesmo diapasão, vale ressaltar que o direito à privacidade e intimidade enquanto direitos de personalidade relacionam-se com os direitos de primeira dimensão[1], isto é, são direitos fundamentais com esteio na filosofia liberal-burguês do século XVIII, os quais se constituem na manifestação da liberdade, e são considerados como direitos de salvaguarda, haja vista exigirem uma não interferência do Estado e uma esfera de autonomia individual frente ao poder estatal. Por esta razão, também são tidos como direitos de caráter negativo, uma vez que exigem uma abstenção - um não fazer por parte do poder público (RUARO, 2013)

Nesta senda, os direitos de personalidade - dentre os quais estão inseridos o direito à intimidade da vida privada - podem ser determinados como direitos subjetivos, privados, absolutos, gerais, extrapatrimoniais, inatos, perpétuos, intransmissíveis, relativamente indisponíveis, possuindo como mote os objetos e expressões internos do indivíduo, com o objetivo de resguardar a integridade e a evolução física e moral da pessoa e forçando todos os sujeitos de direito a abstenções ou a não realizar condutas que de forma ilícita afrontem ou perturbem a personalidade de outra pessoa, sem que incorreram em responsabilidade civil ou, ainda, na subordinação às medidas cíveis apropriadas a impedir a consumação da ameaça ou a mitigar os efeitos da ofensa perpetrada (SOUZA, 1978).

Sob este prisma, resta latente que a tutela desta esfera pessoal do indivíduo (limitada pela intimidade e privacidade) é imprescindível para resguardar-lhe sua realidade enquanto ser

[1] Aqui importante mencionar a crítica feita à divisão geracional dos direitos humanos ou direitos fundamentais. Em razão da construção histórica dos direitos humanos, classificou-os de início em gerações, porém tal classificação se apresenta permeada de atecnia, conforme sustenta Beltramelli Neto (2016, p. 90), para quem não há "sobreposição", "hierarquia" ou "compartimentação" dos direitos humanos, mas tão somente complementação e coexistência de direitos, preferindo-se, portanto, a nomenclatura dimensões. Ainda em relação à classificação em dimensões existem críticas fundamentadas no sentido que ofenderia característica fundamental da estrutura dos próprios direitos, a indivisibilidade. Para Weis (1999, p. 43), "insistir na ideia das gerações, além de consolidar a imprecisão da expressão em face da noção contemporânea dos direitos humanos, pode se prestar a justificar políticas públicas que não reconhecem a indivisibilidade da dignidade humana e, portanto, dos direitos fundamentais".

humano pleno em dignidade. Ademais, a dignidade da pessoa humana, na situação de valor (e princípio normativo) fundante, requer e presume a constatação e defesa dos direitos fundamentais de todas as dimensões, em que pese não todos os direitos fundamentais (ao menos em relação àqueles positivados na Constituição da República Federativa do Brasil de 1988) possuam razão de ser direta no princípio da dignidade da pessoa humana (SARLET, 2010).

Deste modo, circundado em seu espírito com a defesa da dignidade da pessoa humana em quaisquer de seus prismas, o direito brasileiro elenca copiosos institutos de defesa à privacidade e intimidade. Entretanto, esses institutos encontram-se partilhados de forma dispersa no ordenamento brasileiro, não existindo um rol singular de amparo aos mais variados pontos que circundam o direito à privacidade e intimidade.

No tocante ao estudo da não existência de um rol único de amparo à privacidade e intimidade, o fato que deve ser levado em consideração é o de que esses direitos permeiam várias áreas do ordenamento jurídico. Outrossim, as ofensas à privacidade e intimidade podem passar-se em meio virtual, como por exemplo na utilização de dados provenientes da utilização de reconhecimento facial, como também em outros contextos fora daquele ambiente, o que dificulta uma defesa única e singular a tais direitos.

No momento em que se tenta questionar qual o significado semântico da expressão “direitos fundamentais” existem delineações a partir do ponto de vista de que se trata de um sinônimo de “direitos humanos”, particularmente pelo fundamento de que estão a fazer referência ao indivíduo, ainda que retratada por grupos, de tal maneira que, para alguns, seria melhor utilizar-se da terminologia única e geral “direitos humanos”, englobando, de tal modo, os direitos naturais e inalienáveis das pessoas pela sua inerente condição humana, afastando-se, assim, um presumido dualismo de expressões para designar igual categoria (ROSA; FERRARI, 2014).

Entretanto, aconselhável que se faça a devida separação indicando, já de começo, para o fato de que a apesar de os direitos humanos serem a manifestação da condição humana e terem essência universal e de que os direitos fundamentais são, igualmente, sempre direitos humanos (pois também característicos das pessoas), são tidos como fundamentais aqueles que se encontram admitidos e expresso em uma determinada ordem constitucional, já os direitos humanos conservariam guardariam vínculo com diplomas de direito internacional que têm em

vista um valor universal, mas que essencialmente não são considerados por todos os Estados, no entanto, afiguram-se como diplomas diretivos paras esses (SARLET, 2009).

Grande parte da doutrina acredita que as expressões são sinônimas. Refletem, desta forma, uma correlação de gênero e espécie, sendo a intimidade um campo mais restritivo da vida privada. A impropriedade é um atributo ontológico da própria concepção da esfera privada. Assim, resta dificultoso compor uma definição inflexível de intimidade ou de vida privada, tendo em vista a categórica equivocidade de seus limiares, os quais se orientam, como já analisado, pelos preceitos sociais, temporais, culturais e individuais (CRUZ, 2007).

Dessarte, refletir sobre direitos fundamentais é analisar um direito natural do homem que se introduziu ao universo dos direitos humanos considerados como inalienáveis, mas que necessitam de uma ordem constitucional que os preveja e lhes conceda tal característica. Apenas desta forma conseguirão mostrar-se, simultaneamente, como pressuposto, garantia e instrumento do princípio democrático de autodeterminação dos povos através de cada pessoa (SARLET, 2009).

Noutra senda, alguns escolhem delinear uma diferenciação linguística e constitucional de intimidade e vida privada. Vida privada ou vida particular indica aquela distanciada do contato ou do olhar atento de terceiros. Inclui ainda todas as demonstrações que estão separadas da projeção da vida pública da pessoa derivados da função social que cada um detém na sociedade. Aquilo que se pode concluir é que a Carta de 1988 utiliza o conceito “vida privada” com o objetivo de declarar a diferenciação entre as coisas da vida pública e as da vida privada na implementação de balizas - em uma lógica que igualmente é de exclusão (Cruz, 2007).

A intimidade tem uma característica mais restritiva. Faz referência aos fatos e atos mais particulares e pessoais, protegidos em um âmbito de confiança, podendo ser comparado ao conceito estadunidense do *right to be let alone* (DONEDA, 2006).

É justamente nesse contexto que surge a necessidade de defesa à privacidade e intimidade no que tange à utilização de novas tecnologias, mormente, nos dias atuais, o uso do reconhecimento facial, tendo em vista que tal tecnologia não possui regulação no ordenamento jurídico brasileiro, resultando em situação na qual todos – Estado, iniciativa privada e cidadãos – vivenciam grande insegurança jurídica e risco de violações a direitos e garantias fundamentais.

2. INOVAÇÃO TECNOLÓGICA E O RISCO À PRIVACIDADE E À INTIMIDADE: RECONHECIMENTO FACIAL AUTOMATIZADO

Biometria é a área da ciência que determina a identificação de uma pessoa com fundamento em seus atributos físicos, químicos ou comportamentais. Apresenta diversas aplicações em várias áreas, destacando-se mais no campo da segurança, como por exemplo metodologias de gerenciamento de identidade, em que o principal objetivo é verificar a identidade de uma pessoa no contexto de um sistema (JAIN; FLYNN; ROSS, 2008).

O reconhecimento facial é um procedimento biométrico que se constitui em encontrar padrões em atributos faciais como formato do nariz, da boca, do rosto, distância entre olhos, dentre outros.

Uma pessoa tem a capacidade de identificar um indivíduo familiar mesmo através de barreiras como distância, sombras ou somente a visão parcial do rosto. Uma máquina, por outro lado, necessita executar inúmeros procedimentos para encontrar e reconhecer uma série de padrões singulares para identificar um rosto com conhecido ou desconhecido. Com este fim, há técnicas capazes de encontrar, definir e classificar os atributos faciais, resultando em um reconhecimento automático de indivíduos (CINTRA; SILVA, 2015).

A autenticação é o ato de determinar ou atestar alguém, ou alguma coisa, como autêntico, ou seja, que as manifestações realizadas por ou sobre a coisa são verdadeiras. Autenticação biométrica é a utilização da biometria para reconhecimento, identificação ou verificação, de um ou mais atributos biométricos de uma pessoa com o fim de verificar sua identidade. Os sinais biométricos são os traços averiguados pelas metodologias de reconhecimento biométrico BHATTACHARYYA *et al*., 2009).
A metodologia de reconhecimento facial é composta por três processos distintos: Registro, verificação e identificação biométrica. Tais processos se distinguem pela maneira de precisar a identidade de uma pessoa.

O procedimento de registro de dados pessoais e biométricos de uma pessoa em uma aplicação de gerenciamento de identidade é o primeiro passo. A aplicação executa a leitura biométrica,

retira os caracteres que necessitam ser utilizados no reconhecimento facial e os deposita em um banco de dados, junto com a informações pessoais associadas ao indivíduo.

Posteriormente, observa-se o procedimento de reconhecimento biométrico, o qual pode ser executado através de verificação ou identificação. O processo de verificação biométrica consiste na leitura pelo sistema dos dados pessoais, como nomes de usuários, senha, números de identidade, e os biométricos exibidos. A aplicação identifica se os atributos biométricos expostos possuem o mesmo padrão que os atributos biométricos anteriormente guardados para o usuário com os equivalentes dados pessoais. Se a identificação for positiva, a aplicação atesta o usuário como genuíno, caso contrário, a aplicação o atesta como um impostor.

Por fim, o procedimento de identificação biométrica é aquele em que a aplicação realiza a leitura da biometria da pessoa e a coteja com as biometrias anteriormente gravadas, até que o indivíduo seja verificado ou declarado como desconhecido.

Em outras palavras, o reconhecimento facial inicia-se com coleta da imagem de uma pessoa. Um filtro identifica se o atributo recuperado é uma face ou não. Após, é efetuada uma normalização, em que os indivíduos são classificados em padrões. Na próxima etapa, os atributos e caracteres da face são remodelados em pontos de referência, os quais são verificados. Esse agrupamento de dados é trabalhado como um identificador vinculado àquele indivíduo. Em um serviço de verificação, por exemplo, a câmera filma ou registra uma imagem e a aplicação do sistema procura no banco de dados se há algum rosto com determinado grau de afinidade.

A maioria dos instrumentos revolucionários na área da tecnologia advém de uma evolução disruptiva que, no mesmo contexto em que facilita o aparecimento de alguma atividade específica, desperta várias consequências reflexas jamais imagináveis, as quais alteram de forma efetiva o relacionamento do homem com o meio, como por exemplo o reconhecimento facial.

Nesse sentido, a dificuldade em prever as consequências futuras retrata uma das principais características da inovação tecnológica, uma vez que apenas se compreenderão todos os seus impactos diretos e indiretos depois de sua contextualização sociocultural (MISUGI; FREITAS; EFING, 2016).

Nesta senda, para elucidar tal argumentação interessante mencionar a obra paradigmática de Warren e Brandeis, *The right to privacy*, de 1890, na qual se vaticinou que os lugares sagrados da vida íntima e doméstica teriam sido profanados pelas fotografias instantâneas e produções jornalísticas, de maneira que aquilo que outrora sussurrado na intimidade de um closet passaria a ser anunciado nos terraços das residências. (WARREN; BRANDEIS, [2019]).

Segundo alguns autores, a tecnologia de reconhecimento facial tem como objetivo combinar as desenvolvidas percepções humanas com a imensa capacidade de processamento e armazenamento dos computadores, utilizando-se, para isso, de algoritmos computacionais (WELINDER, 2012).

Ademais, a tecnologia de reconhecimento facial utiliza uma câmera fotográfica ou filmadora atrelada a uma aplicação/software de reconhecimento facial. Este *software* tem a capacidade de identificar e isolar faces humanas capturadas através da câmera e analisá-las utilizando um algoritmo que extrai e verifica os atributos. O algoritmo verifica e mensura 'pontos nodais' no rosto, o quais são ajustados pelos picos e vales que formam as características da face humana. Fazendo uso destas medições, o algoritmo verifica os atributos de identificação de uma pessoa, tais como a distância entre as orelhas, do nariz, a forma das maçãs do rosto, e o tamanho da linha da mandíbula (LEVASHOV, 2013).

Destaque-se, por absolutamente oportuno, que este assunto retrata uma discussão que tende a tornar-se cada vez mais importante, quer pela capacidade de processamento das novas aplicações, quer pelo número de imagens que são postadas *online*. Como exemplo, no ano de 2000, cerca de 100 bilhões de fotos foram tiradas ao redor do globo. Após pouco mais de uma década, em 2012, somente no *Facebook* foram postadas 300 milhões de fotos a cada dia, com a marcação de 100 milhões de indivíduos diariamente, fornecendo uma base de dados com imagens de faces de bilhões de pessoas, correlacionando-a ainda aos caracteres pessoais, locais, datas e horas de cada imagem (ACQUISTI; GROSS; STUTZMAN, 2014).

Ademais, poder-se-ia também mencionar, as 75 milhões de fotografias em poder do departamento do Estado norte-americano, ou ainda a base de armazenamento do *Flickr*, com 3,4 bilhões de fotos, ou, por fim, os 7,2 bilhões na base da *Photobucket*. Introduz-se, desta maneira, uma apreensão jurídica compreendendo o reconhecimento e identificação facial, uma

vez que, embora realize esta relação entre as informações virtuais e o ambiente físico a que se dispõe, pode resultar em danos aos direitos dos cidadãos e consumidores (LEVASHOV, 2013).

Ressalta-se que o risco à privacidade e à intimidade não se limitam mais às inter-relações de consumo propriamente ditas, ou às condutas comerciais abrangendo determinado produto ou serviço, haja vista que qualquer indivíduo que transita em um espaço público (e até mesmo privado) pode ser objeto de investigações instantâneas e completas, através, por exemplo, do uso de sistemas de reconhecimento facial.

Como mencionado alhures, por referir-se a uma inovação tecnológica, ainda não se pode mensurar todas as consequências que do reconhecimento facial podem resultar, havendo apenas um delineamento do seu potencial para o bem ou para o mal, como a reconhecimento de terroristas em uma multidão, contexto de combate a fraudes e estelionato, dentre outros (MISUGI; FREITAS; EFING, 2016).

Diante de tal contexto, em 2012, Al Franken, senador norte-americano, iniciou tratativas com o *Facebook* e o FBI para que fosse reavaliado o uso desta tecnologia de reconhecimento facial, deixando claro, desta forma, a imprescindibilidade de atuação do Estado frente a esta inovação e seu relacionamento com o meio virtual, até mesmo com uma readequação dos direitos fundamentais e da personalidade dos cidadãos, conjugando-as ademais com as vantagens e as ameaças do desenvolvimento tecnológico (LEVASHOV, 2013).

O Brasil possui 37 iniciativas em municípios fazendo uso, de alguma forma, de aplicações de reconhecimento facial. Dezenove destes projetos foram iniciados no interregno de 2018 a 2019. Essas iniciativas, em geral, são implementadas, mormente, nas áreas de segurança pública, transporte e controle de fronteiras (AGÊNCIA BRASIL, 2019).

A utilização de reconhecimento facial tornou-se particularmente popular em 2019. Durante o Carnaval, as cidades do Rio de Janeiro e de Salvador tornaram-se o centro de implantação da tecnologia de reconhecimento facial. Ademais, o ano de 2019 pautou, no mínimo, três audiências públicas, sendo duas na Câmara dos Deputados e uma coordenada pelo Ministério Público do Distrito Federal e Territórios (MPDFT) (INSTITUTO IGARAPÉ, 2019).

Bases de dados públicas e privadas (algumas possuindo dados detalhados a respeito da vida civil e penal dos cidadãos) já recolhiam informações faciais e biométricas mesmo antes do Brasil aprovar a sua lei de proteção de dados pessoais. Tais bases de dados são essenciais para abastecer o sistema de reconhecimento facial com atributos que possam indicar quando um indivíduo possui pendências junto às autoridades, apontamento criminal ou quando não é quem diz ser.

Assim, diante do aumento dessas tecnologias e dos perigos que possam podem manifestar, urge a necessidade que se avance na agenda de um debate público profuso e informado a respeito de onde e como esta tecnologia pode ou deve ser aplicada. Nesse sentido, faz-se necessária uma regulação e uso adequado desse tipo de tecnologia, com fundamento princípios (tais como proporcionalidade, finalidade, consentimento e transparência) para orientar sua utilização e para resguardar o desempenho direitos (como por exemplo, o direito de ir e vir, de liberdade de expressão, à privacidade e à intimidade) e liberdades dos cidadãos.

3. A REGULAÇÃO DO RECONHECIMENTO FACIAL NO BRASIL

Não se pode olvidar que o desenvolvimento tecnológico possibilita uma maneira cada vez mais rápida de recepção e captação e o armazenamento de dados. Dentre as várias inovações que modificaram de maneira efetiva os hábitos da sociedade, a internet vislumbra-se como uma das mais importantes. A sua função rede de dados ilimitados e como mecanismo de comunicação e acercamento dos indivíduos é diretamente proporcional ao aumento das chances de danos às liberdades individuais, em destaque à intimidade e à privacidade.

A utilização nociva da tecnologia no âmbito deste direito fundamental conduz-se a identificar maneiras de controlar o acesso à dados sobre a pessoa e a destinação que se faz deles. Em que pese a falta de regramento específico que regulamente a criação, a utilização e a manutenção do uso de reconhecimento facial, a ordem jurídica brasileira dispõe de bases principiológicas que buscam assegurar o amparo à a intimidade e à privacidade.

Nesta vereda, no presente trabalho, buscou-se identificar a atual abordagem que o regramento jurídico brasileiro confere à privacidade e à intimidade, indicando evoluções e obstáculos, mormente quando tais direitos se veem em risco de serem lesionados pela utilização de novas tecnologias, como por exemplo o reconhecimento facial automatizado.

As inovações tecnológicas convertem a informação em um bem fundamental da sociedade atual. A utilização de algoritmos e aplicações interativas produzem um novo produto. A pessoa oferece as informações de uma forma repentina e espontânea e, por consequência, após estes serem armazenados, ignora-se de que os declarou. Por esta razão, é uma dificuldade possibilitar amparo à privacidade e à intimidade no tocante a esses serviços (ZENCOVICH, 1984).

Os dados coletados representam características da personalidade e expõem comportamentos e preferências, viabilizando até mesmo delinear um perfil psicológico da pessoa. Desta forma, há possibilidade de se identificar hábitos de consumo, que possuem grande relevância para a propaganda e o comércio. É possível, através destes dados, confeccionar uma imagem completa e pormenorizada do indivíduo, que se poderia designar de características de personalidade, inclusive na seara da intimidade. O indivíduo transforma-se no denominado "homem de cristal" (LIMBERGER, 2009).

As formas interativas de comunicação transformam capacidade de coleta de informações, estabelecendo uma comunicação eletrônica constante e direta entre os administradores dos novos serviços e os usuários. Assim, existe a possibilidade não apenas de um monitoramento do comportamento dos usuários, mas igualmente um entendimento mais acurado de seus costumes, inclinações, interesses e gostos. Desse contexto, provém a possibilidade de todo um conjunto de utilizações secundárias dos dados coletados.

Nesse sentido, os bancos de dados vêm sendo utilizados com finalidades diversas, que vão desde o armazenamento de informações corriqueiras, como o nome e o endereço do usuário, para ajudar na sua identificação nos relacionamentos com fornecedores de bens e serviços, até a combinação de informações mais complexas para delinear uma descrição precisa do usuário, de seus hábitos, gostos e preferências. O uso de informações pessoais pode prestar-se a diversos fins objetivos, como publicitários, políticos e até persecutórios, podendo, desta forma, ferir de ilicitude a sua utilização desvirtuada (CRUZ, 2007).

Depois da aprovação da Regulamentação Geral de Proteção de Dados (GDPR) pela União Europeia e o escândalo envolvendo a Cambridge Analytica, tornou-se ainda mais latente a necessidade de o Brasil editar legislação de proteção de dados mais aprofundada, visando a

nortear a coleta, uso, armazenamento e processamento de dados entre entres públicos e privados, bem como se enquadrar no padrão internacionalmente exigido.

A edição de um regramento específico de proteção de dados traz, ademais, relação com o intento de o Brasil pleitear sua entrada na Organização para a Cooperação e desenvolvimento Econômico (OCDE) (KUJAWSKI; THOMAZ, 2018). Isso porquanto, a mencionada instituição dispõe de diretrizes e orientações a respeito do tema desde 1980 e, em 2013, as atualizou para readequá-las ao atual nível da sociedade de informação. Conquanto as diretrizes da OCDE não possuam força de lei, configuram-se em requisitos para a admissão de novos membros, sendo fundamental para o Brasil a aprovação de normas mais robusta em relação ao tema. (MONTEIRO, 2018).

Nessa conjuntura, em 14 de agosto de 2018, foi sancionada a Lei Federal nº 13.709/2018, conhecida como Lei Geral de Proteção de Dados (LGPD), a qual se impõe a qualquer operação de tratamento realizada por pessoa natural ou por pessoa jurídica de direito público ou privado, independentemente do meio, do país de sua sede ou do país onde estejam localizados os dados, salvo exceções estipuladas em seu artigo 4º (BRASIL, 2019).

A relevância atribuída ao momento de promulgação deste normativo parece corroborar e fortalecer a propensão de reputar a privacidade como fundamental ao desenvolvimento das relações sociais na conjuntura de um Estado Democrático de Direito contextualizado em um agrupamento social informacional (DIVINO; MAGALHÃES, 2019).

Vale mencionar que diante da crise pandêmica causada pela COVID-19 (Coronavírus), houve grande movimentação para que fosse adiada a vigência da LGPD, especialmente em razão da preocupação com as sanções previstas na lei.

Obviamente que a coleta de dados pessoais e a proteção destes é importante a qualquer tempo. Ocorre que a necessidade de transparência acerca da finalidade e tratamento destinado a estes dados é de fundamental importância em um momento de grave crise pandêmica. A título de exemplo, cita-se a utilização do geoprocessamento para avaliar a mobilidade populacional, eventuais pontos de aglomeração e, com isso, a adesão da sociedade ao isolamento social.

Destaca-se ainda que o Governo Federal publicou em 17 de abril a Medida Provisória 954/2020 (BRASIL, 2020), dispondo sobre o compartilhamento de dados por empresas de telecomunicações com o Instituto Brasileiro de Geografia e Estatística (IBGE), visando a realização de entrevistas não presenciais no desenvolvimento de pesquisas domiciliares.

Tais medidas, direta ou indiretamente relacionadas ao combate da pandemia, necessitam de regulação, principalmente do processo de coleta desses dados pessoais. Vieira (2019) destaca que a LGPD ao longo do processo de utilização da informação, veda que o titular de tais dados seja identificado ou identificável.

Inicialmente foi editada a Medida Provisória 959/2020 (BRASIL, 2020), determinando que o início de vigência da LGPD ocorresse em maio de 2021. Porém, no dia 19 de maio de 2020 o Senado Federal aprovou o PL 1.179/20, que entre outras questões tratou da manutenção da vigência da LGPD para seu prazo original, ou seja, agosto de 2020, prorrogando-se apenas as aplicações de sanções previstas na lei para agosto de 2021. Parece evidente a importância de vigência da LGPD no mais breve período de tempo possível, dada a relevância das matérias tratadas.

Importante destacar as definições de dados pessoais, inseridas no artigo 5º, sendo considerados de forma apartada os dados pessoais, que são aqueles que consistem em informação relacionada a pessoa natural identificada ou identificável e dados sensíveis, por outro lado, aqueles que consistem em dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural. A análise de informações pessoais apenas poderá ocorrer atendendo a autorização prévia, gratuita, informada e inequívoca do titular e, no caso de dados sensíveis, a mencionada permissão deverá ainda incluir-se como cláusula própria, separa das demais.

Nesta esteira, são identificados como dados sensíveis, aquelas informações cuja análise possa resultar em atos discriminatórios do titular, como aquelas informações que demonstrem a origem racial ou étnica, as convicções religiosas, filosóficas ou morais, os pontos de vista políticos, a filiação sindical, partidária ou a organizações de caráter religioso, filosófico ou político, os atinentes à saúde e à vida sexual, assim como os dados genéticos e biométricos.

Relevante mencionar o resultado positivo sobre a defesa aos direitos fundamentais à privacidade e à intimidade que a delimitação de "dados sensíveis" poderá resultar. Isto é, a mencionada delimitação possibilita uma defesa ativa sobre as informações consideradas sensíveis por apresentarem características da pessoa que esta provavelmente não gostaria que divulgassem por estarem no âmbito privado ou íntimo de sua vida, circunstância sobre a pessoal que – muito provável – ela guarde somente para os indivíduos de seu convívio particular. A exposição inadequada ou não chancelada desse tipo de informação é indubitavelmente uma ofensa explícita aos direitos fundamentais à privacidade e à intimidade, uma vez que reverberam de modo direito na figura produzida pela sociedade a respeito de determinada pessoa.

Assim, a criação de estereótipos pode, em situações de exposição de informações sensíveis sem concordância, figurar atributos que a pessoa em sua livre escolha não pretendeu que fossem exibidos. Ademais, em situações extremas, revelar atributos que lhe torne vítima de transgressões de outros direitos constitucionais, assim como é a discriminação em seus mais variados aspectos. Nesse diapasão, quando se trata da regulação do reconhecimento facial, o debate é deveras incipiente, em que pese a massiva e exploratória implementação desta tecnologia.

Especialistas pontuam que a Lei Geral de Proteção de Dados Pessoais traz critérios, no entanto, ainda existe a necessidade de um debate em relação a quais tipos de informações pessoais devem, de fato, ser consideradas públicas e, dessa forma, ficar disponibilizadas para toda a sociedade. A esperança é de que a Autoridade Nacional de Proteção de Dados (ANPD), juntamente com a sociedade, regule, sane dúvidas e detalhe a questão (SERPRO, 2019).

A Autoridade Nacional de Proteção de Dados foi criada pela Lei nº 13.853, de 8 de julho de 2019 e, consoante tal norma, estão, dentre as atribuições da ANPD, zelar pela proteção dos dados pessoais, elaborar diretrizes para a Política Nacional de Proteção de Dados Pessoais e da Privacidade e aplicar sanções em casos de tratamento de dados realizado de maneira irregular (BRASIL, 2019).

Mesmo assim, alguns doutrinadores defendem que diante do uso de dados biométricos, tem-se um cenário em que se demanda uma regulamentação de maneira direta para que se acautele a ameaça que se apresenta (LEVASHOV, 2013).

Noutra senda, ressalte-se a construção teórica concebida por Thierer (2015, p. 39-40), em que se reflete precisamente os valores e ameaças abrangendo uma política pública de controle tecnológico, apontando duas teorias: *permissionless innovation* e *the precautionary principle*. Compreende-se por *permissionless innovation* o entendimento de que se deve efetuar o experimento de novas tecnologias e atividades mercadológicas sem a imposição de aprovação prévia, salvo fique evidente que sua aplicabilidade prática contraria o arcabauço jurídico vigente. No tocante ao *the precautionary principle*, a lógica é invertida, impondo que os criadores e usuários de determinada inovação tecnológica demonstrem sua segurança e conformação. Em resumo, o autor assinala a indispensabilidade de um controle democrático no que se refere a implementação de novas tecnologias.

Importante ressaltar que uma regulamentação escorreita, seja de forma preventiva ou na apreciação de eventual responsabilidade, é significativamente desafiadora devido a imprecisão na concepção de privacidade, haja vista representar valor subjetivo e de árdua compreensão.

No ordenamento jurídico brasileiro, por exemplo, estranhamente, não é encontrado o termo privacidade na Constituição Federal, no Código Civil e nem mesmo no Código de Defesa do Consumidor, sendo alçado, mesmo assim, a direito fundamental uma vez que, consoante art. 5º, inc. X, são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação (MISUGI; FREITAS; EFING, 2016).

Já a Lei Geral de Proteção de Dados, Lei nº 13.709/2018, que tem dentre seus objetivos a proteção aos direitos fundamentais de liberdade e de privacidade, passou a utilizar o termo privacidade, também como fundamento no disciplinamento da proteção de dados pessoais no Brasil. Ademais, de acordo com a LGPD, toda pessoa natural tem assegurada a titularidade de seus dados pessoais e garantidos os direitos fundamentais de liberdade, de intimidade e de privacidade.

Refere-se, neste contexto, às informações depositadas em bancos de dados digitais, cujo aumento desenfreado tem sido uma das grandes dificuldades enfrentadas pelos consumidores hodiernamente, e que infringe o que se tem convencionado designar de “direito à autodeterminação informacional” (ou “liberdade informática”, na Alemanha ou, ainda,

"proteção de dados pessoais", como na Itália), compreendido como o direito de o indivíduo tomar conhecimento a respeito do armazenamento e utilização de seus dados por terceiros, assim como controlar ou mesmo impedir o uso de tais informações. A reprodução será considerada lesiva ou não se levando em consideração dois fatores: o tipo de informação divulgada e a maneira sua divulgação (BARBOSA, 2013).

Não obstante, conservar-se uma justificada nébula em relação ao conceito e fronteiras da privacidade em face de sua abrangência e dinamicidade, que pode ser tido como relacionado ao da própria vida, considerando-se como reflexo ou revelação deste. Por certo, o termo não é preciso. Destarte, prefere-se utilizar a terminologia direito à privacidade, com um significado aberto e geral, com o objetivo de abranger todas essas expressões do campo da intimidade, privacidade e da personalidade, as quais são consagradas pelo texto constitucional (SILVA, 2010).

Outrossim, concebe-se a privacidade como o agrupamento de dados relacionados à pessoa que ela poderia resolver conservar sob o seu privativo domínio, ou compartilhar, definindo a quem, quando, onde e em que situações, sem que a isso pudesse ser legalmente compelido. O campo da inviolabilidade, dessarte, é amplo, compreende a esfera da vida doméstica, dos relacionamentos em família e afetivos como um todo, eventos, hábitos, lugares, nome, imagens, pensamentos, segredos, e, do mesmo modo, as origens e projetos futuros da pessoa (SILVA, 2010).

Tal conceito guarda estreita relação com designado *right to be alone*, que é o direito de todo indivíduo adotar sozinho as disposições no campo de sua vida privada. Nesse sentido, tal direito de ser deixado só, em paz, embora profundamente privatista, vem a proclamar o adequado poder da atuação política da pessoa enquanto cidadã, no contexto em que deseja resguardar uma seara privada indisponível e inacessível, a não ser pela escolha de seu único detentor, de acordo com os interesses sociais que desta situação emergem, atualmente concebendo verdadeira 'liberdade democrática (EFING, 2002).

Desse modo, refere-se a um direito fundamental que se configura indispensável à vida digna e concepção da personalidade do indivíduo, constituindo imprescindível para o completo exercício da cidadania e de outras liberdades, compreendendo também concepção ampla que abrange o direito à intimidade, à vida privada e à imagem.

Assim, em que pese todo o esclarecimento doutrinário, mormente diante das diversas inovações tecnológica, característica de uma atual sociedade da informação, pode-se perceber uma mitigação no amparo à privacidade, como por exemplo, em relação à utilização de tecnologias de reconhecimento facial automatizado, as quais necessitam de maior cuidado e dedicação pelos operadores do Direito e pelos formadores de políticas públicas.

CONSIDERAÇÕES FINAIS

Como demonstrado no presente trabalho, o reconhecimento facial não apenas coleta e armazena informações biométricas do indivíduo, mas, em verdade, consiste em uma aplicação tecnológica com capacidade de controlar e vigiar cidadãos e direitos e, por conseguinte, oferecer sério risco de lesão aos direitos à privacidade e à intimidade.

Nesse sentido, a ausência de regulação específica e de um aprofundamento do debate entre a sociedade, a iniciativa privada e os formadores de políticas públicas a respeito da utilização e consequências do reconhecimento facial, podem resultar em um controle policial desarrazoado, em um sistema de monitoramento em massa e, por derradeiro, na mitigação de direitos e liberdades constitucionalmente garantidas, enfraquecendo, sobremaneira, os pilares sob os quais repousa o atual Estado Democrático de Direito.

Por fim, tem-se que o crescente interesse de governos, de empresas e da sociedade nos benefícios esperados da utilização de reconhecimento facial é acompanhado por uma – ainda incipiente – discussão a respeito da privacidade e da proteção de dados.

REFERÊNCIAS BIBLIOGRÁFICAS

ACQUISTI, Alessandro; GROSS, Ralph; STUTZMAN, Fred. **Face recognition and privacy in the age of augmented reality**. Journal of Privacy and Confidentiality, v. 6, n. 2, 2014. Disponível em: https://journalprivacyconfidentiality.org/index.php/jpc/article/view/638. Acesso em: 10 fev. 2020.

AGÊNCIA BRASIL. **Tecnologias de Reconhecimento Facial São Usadas em 37 Cidades no País**. Disponível em: http://agenciabrasil.ebc.com.br/geral/noticia/2019-09/tecnologias-de-reconhecimento-facial-sao-usadas-em-37-cidades-no-pais. Acesso em: 25 dez. 2019.

BARBOSA, Fernanda Nunes. **Informação e consumo: a proteção da privacidade do consumidor no mercado contemporâneo da oferta**. Revista de Direito do Consumidor, São Paulo, v. 22, n. 88, p. 103-143, jul. 2013. p. 151.

BELTRAMELLI NETO, Silvio. **Direitos Humanos**. 3. ed. Salvador: JusPODIVM, 2016.

BHATTACHARYYA, D.; RANJAN, R.; ALISHEROV, F. A.; CHOI, M. **Biometric authentication: A review**. International Journal of u- and e-Service, Science and Technology, 2009.

BRASIL. **Constituição da República Federativa do Brasil de 1988**. Brasília, DF: Presidência da República, [2019]. Disponível em: http://www.planalto.gov.br/ccivil_03/Constituicao/ Constituiçao.htm. Acesso em: 11 fev. 2020.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Brasília, DF: Presidência da República, [2019]. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 20 dez. 2019.

BRASIL. **Lei nº 13.853, de 8 de julho de 2019**. Brasília, DF: Presidência da República, 2019. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/lei/l13853.htm. Acesso em: 20 dez. 2019.

BRASIL. **Medida Provisória nº 954, de 17 de abril de 2020**. Dispõe sobre o compartilhamento de dados por empresas de telecomunicações prestadoras de Serviço Telefônico Fixo Comutado e de Serviço Móvel Pessoal com a Fundação Instituto Brasileiro de Geografia e Estatística, para fins de suporte à produção estatística oficial durante a situação de emergência de saúde pública de importância internacional decorrente do coronavírus (covid-19), de que trata a Lei nº 13.979, de 6 de fevereiro de 2020. Brasília, DF: Presidência da República, 2020. Disponível em: http://www.planalto.gov.br/CCIVIL_03/_Ato2019-2022/2020/Mpv/mpv954.htm. Acesso em: 10 mai. 2020.

BRASIL. **Medida Provisória nº 959, de 29 de abril de 2020**. Estabelece a operacionalização do pagamento do Benefício Emergencial de Preservação do Emprego e da Renda e do benefício emergencial mensal de que trata a Medida Provisória nº 936, de 1º de abril de 2020, e prorroga a **vacatio legis** da Lei nº 13.709, de 14 de agosto de 2018, que estabelece a Lei Geral de Proteção de Dados Pessoais – LGPD. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/mpv/mpv959.htm. Acesso em: 10 mai. 2020.

CRUZ, Marco Aurélio Rodrigues da Cunha e. **A disciplina normativa brasileira sobre a intimidade e os bancos de dados**. Araucaria. Revista Iberoamericana de Filosofía, Política y Humanidades, vol. 9, núm. 18, 2007, pp. 56-84, Universidad de Sevilla Sevilla, España.

DA ROSA, Tais Hemann; FERRARI, Graziela Maria Rigo. **Privacidade, intimidade e proteção de dados pessoais**. Argumenta Journal Law, Jacarezinho - PR, n. 21, p. 137-166, fev. 2015. ISSN 2317-3882. Disponível em: http://seer.uenp.edu.br/index.php/argumenta/article/view/495. Acesso em: 15 nov. 2019.

DIAS, Eduardo Rocha; ROCHA, Ronald Fontenele. A constituição líquida: mutação constitucional e expansão de Direitos fundamentais na hipermodernidade. **Revista de Direitos Fundamentais & Democracia**, Curitiba, v. 24, n. 1, p.143-160, jan/abr, de 2019. Disponível em: https://revistaeletronicardfd.unibrasil.com.br/index.php/rdfd/article/view/1423/573. Acesso em: 10 fev. 2020.

DIVINO, Sthéfano Bruno Santos. MAGALHÃES, Rodrigo Almeida. A proteção de dados e direito de personalidade da pessoa jurídica: reflexões sob a ótica da Lei nº 13.709/2018. **ARGUMENTUM**: Revista de Direito da Universidade de Marília. Marília: UNIMAR, v. 20, n. 3, pp. 915-929, set.-dez. 2019.

DONEDA, Danilo. **Da privacidade à proteção dos dados pessoais**. Rio de Janeiro: Renovar, 2006

EFING, Antônio Carlos. **Banco de dados e cadastro de consumidores**. São Paulo: Revista dos Tribunais, 2002.

FACCHINI NETO, Eugênio. **Reflexões histórico-evolutivas sobre a constitucionalização do direito privado**, in SARLET, Ingo Wolfgang (org.). Constituição, Direitos Fundamentais e Direito Privado. Porto Alegre: Liv. Do Advogado, 2003, p. 11-60.

INSTITUTO IGARAPÉ. **Reconhecimento Facial do Brasil**. Rio de Janeiro, 2019. Disponível em: https://igarape.org.br/infografico-reconhecimento-facial-no-brasil/ Acesso em: 10 dez. 2019.

JAIN, Anil K.; FLYNN, Patrick; ROSS, Arun A. Handbook of Biometrics. Springer US, 2008. Disponível em: http://www.springer.com/us/book/9780387710402. Acesso em: 10 nov. 2019.

KARAM, Maria Lúcia. **Escritos sobre a Liberdade**. Volume 4: Liberdade, intimidade, informação e expressão, Rio de Janeiro: Lumen Juris, 2009, p. 31.

KUJAWSKI, FF; THOMAZ, ACE. **The Privacy, Data Protection and Cybersecurity**. Law Review 5th Edition, October/2018, p. 1.

LEVASHOV, Kirill. **The Rise of a New Type of Surveillance for Which the Law Wasn't Ready**. Columbia Science and Technolog y Law Review, v. 15, p. 164, fall 2013. Disponível em: http://stlr.org/volumes/volume-xv-2013-2014/the-rise-of-a-new-type-of-surveillance-for-which-the-law-wasnt-ready/. Acesso em 14 nov. 2019.

LIMBERGER, Têmis. **Da evolução do Direito a ser deixado em paz à proteção dos dados pessoais**. Revista Novos Estudos Jurídicos. Vol. 14, n° 2, p. 27-53, 2009. Disponível em: https://siaiap32.univali.br/seer/index.php/nej/article/view/1767. Acesso em 25 out. 2019.

MISUGI, Guilherme; FREITAS, Cinthia O. de Almeida; EFING, Antônio Carlos. **Releitura da Privacidade Diante das Novas Tecnologias: Realidade Aumentada, Reconhecimento Facial e Internet das Coisas**. Revista Jurídica Cesumar, Maringá - PR, v. 16, p. 427-453, maio/ago. 2016. Disponível em: http://dx.doi.org/10.17765/2176-9184.2016v16n2p427-453. Acesso em: 15 nov. 2019.

MONTEIRO, RL. **Lei Geral de Proteção de dados: análise**. [s.i], 18 jul. 2018. Disponível em: https://baptistaluz.com.br/institucional/lei-geral-de-protecao-de-dados-do-brasil-analise/. Acesso em: 20 out. 2019.

RUARO, Regina Linden. **O Direito Fundamental à Privacidade e à Intimidade no Cenário Brasileiro na Perspectiva de um Direito à Proteção de Dados Pessoais** – publicação conjunta com alunos do mestrado: Andrey Felipe Lacerda Gonçalves, Monique Bertotti e Veyzon Campos Muniz. Revista dos Tribunais on line - Revista de Direito Privado, vol, 54, p. 45/56. abr. 2013, DRT/2013/3870.

SARLET, Ingo Wolfgang. **A eficácia dos direitos fundamentais: uma teoria geral dos direitos fundamentais na perspectiva constitucional**. 10. ed. ver. atual. e ampl. Porto Alegre: Livraria do Advogado, 2009

SARLET, Ingo Wolfgang. **Dignidade da Pessoa Humana e Direitos Fundamentais**. Porto Alegre: Livraria do Advogado, 2010, p. 97.

SERVIÇO FEDERAL DE PROCESSAMENTO DE DADOS – SERPRO. **O Que Muda Com a Lei Geral de Proteção de Dados Pessoais**. Brasília, 2019. Disponível em: https://www.serpro.gov.br/lgpd/menu/a-lgpd/o-que-muda-com-a-lgpd. Acesso em: 15 out. 2019.

SILVA, Alex Lima; CINTRA, Marcos Evandro. **Reconhecimento de padrões faciais: Um estudo**. In: Encontro Nacional de Inteligência Artificial e Computacional, 2015, Proceedings ENIAC, 224-231, 2015.

SILVA, Edson Ferreira da. **Direito à Intimidade: de acordo com a doutrina, o direito comparado, a Constituição de 1988 e o Código civil de 2002**. 2 ed. São Paulo: Editora Juarez de Oliveira, 2003.

SILVA, José Afonso da. **Curso de direito constitucional positivo**. 33. ed. São Paulo: Malheiros, 2010, p. 206.

SOUZA, Rabindranath Capelo de. **A Constituição e os direitos de Personalidade**. In: MIRANDA, Jorge (coord.). Estudos sobre a Constituição. 2º v. Lisboa: Petrony, 1978, p. 93.

THIERER, Adam D. **The internet of things and wearable technology: addressing privacy and security concerns without derailing innovation**. Richmond Journal of Law & Technology, v. 21, n. 2, 2015. Disponível em: https://scholarship.richmond.edu/jolt/vol21/iss2/4/. Acesso em: 5 nov. 2019.

VIEIRA, E. L. C. A proteção de dados desde a concepção (by design) e por padrão (by default). *In:* Maldonado, V. N. (Coord.). **LGPD: Lei Geral de Proteção de Dados pessoais: manual de implementação**. São Paulo, Thomson Reuters Brasil, 2019.

WARREN, Samuel D.; BRANDEIS, Louis D. **The Right to Privacy**. Harvard Law Review, v. 4, n. 5, 1890. Disponível em: http://faculty.uml.edu/sgallagher/Brandeisprivacy.htm. Acesso em: 10 nov. 2019.

WEIS, Carlos. **Direitos Humanos Contemporâneo**. 1. ed. São Paulo, Malheiros, 1999.

WELINDER, Yana. **A face tells more than a thousand posts: developing face recognition privacy in social networks**. Harvard Journal of Law & Technolog y, Boston, v. 26, n. 1, fall 2012. Disponível em: http://jolt.law.harvard.edu/articles/pdf/v26/26HarvJLTech165.pdf. Acesso em 12 nov. 2019.

ZENCOVICH, Vincenzo Zeno. **I nuovi sistemi telematici interattivi e la tutela del diritto all'identità personales**, QDC, In: Banche Dati Telematica e Diritti della Persona, CEDAM, Padova, 1984.