DIREITO COMPARADO E INTELIGÊNCIA ARTIFICIAL: A RESPONSABILIZAÇÃO CIVIL DO RECONHECIMENTO FACIAL NA LGPD

COMPARATIVE LAW AND ARTIFICIAL INTELLIGENCE: CIVIL LIABILITY FOR FACIAL RECOGNITION IN LGPD

Daniela Kojiio Nobre*

Resumo: Direito e Inteligência Artificial (IA) são áreas que devem ser aproximadas. Assim, o ponto principal desta pesquisa, a partir das informações divulgadas pela administração pública europeia, é o estudo sobre os desafios que a definição de reconhecimento facial na LGPD irá trazer, especialmente no campo da responsabilização civil. A metodologia utilizada será o método indutivo cujo objetivo é chegar a conclusões mais amplas do que o conteúdo estabelecido pelas premissas de base. O procedimento de pesquisa será do tipo pesquisa descritiva aplicando a técnica de coleta de dados chamada análise bibliográfica. E as conclusões não são buscadas de forma apriorística, logo, elas devem resultar da análise de fenômenos recorrentes. Por fim, este trabalho irá sugerir uma definição de reconhecimento facial para suprir esse vácuo legislativo e, uma vez que a LGPD não estabelece o reconhecimento facial e como um setor específico de uso da IA.

Palavras-chave: Inteligência artificial. LGPD. Reconhecimento facial..

Abstract:
Law and Artificial Intelligence (AI) are areas that must be approximated. Thus, the main point of this research, based on information released by the European public administration, is the study on the challenges that the definition of facial recognition in LGPD will bring, especially in the field of civil liability. The methodology used will be the inductive method whose objective is to reach conclusions broader than the content established by the basic premises. The research procedure will be of the descriptive research type using the data collection technique called bibliographic analysis. And the conclusions are not sought a priori, so they must result from the analysis of recurring phenomena. Finally, this work will suggest a definition of facial recognition to fill this legislative vacuum and, since the LGPD does not establish facial recognition and as a specific sector for the use of AI.Keywords: artificial intelligence. LGPD. facial recognition.

Keywords: *Artificial intelligence. LGPD. Facial recognition.*

* Graduada em Relações Internacionais pela Universidade Federal da Santa Catarina (UFSC) em 2015. Graduanda em Direito pela Universidade Federal de Santa Catarina (UFSC). Pesquisadora do Grupo de Pesquisa Direito, Racionalidade e Inteligencia Artificial (UNB) Lattes: lattes.cnpq.br/9682512923620902. dknobre@gmail.com

INTRODUÇÃO

Visando alcançar o Estado da Arte da entre Direito e Inteligência Artificial (IA) é necessário suprir algumas lacunas científicas. Considerando Direito e Inteligência Artificial (IA) áreas aparentemente distantes, é possível identificar seu encontro na Estratégia Nacional de Inteligência Artificial quando trata do tópico Legislação, Regulação e Uso Ético da Inteligência Artificial. É importante salientar que o Ministério da Ciência, Tecnologia, Inovações e Comunicações (MCTIC), lançou a consulta pública desta Estratégia Nacional de Inteligência artificial para que potencialize os benefícios que a IA, mitigando eventuais impactos negativos, e esta consulta ficou disponível no portal Participa.br entre os dias 12 de dezembro de 2019 até 02 de março de 2020

Para introduzir este tema, será apresentado uma análise das referências de pesquisa dos últimos anos. Em termos de pesquisa científica, Almada (2020) aproxima Filosofia do Direito e Inteligência Artificial ao realizar uma revisitação sobre seus principais autores. Este autor verifica que as tecnologias que utilizam IA estão ocupando um espaço nas sociedades modernas e alterando dinâmicas sociais que irão ensejar a necessidade de criação de novos modelos de relações. Essas mudanças impactarão os sistemas normativos, especialmente quando for realizado a automatização de funções que eram realizadas por juízes, advogados e operadores do direito. Por isso ele apresenta um diálogo entre os principais autores da temática e demonstra que as duas áreas precisam de compartilhar informações. Essa aproximação poderá ocasionar uma mudança de paradigma, não apenas por causa das diferenças metodológicas entre as áreas, mas pela própria troca de contribuições multidisciplinares que envolvem ramos das ciência supostamente separados.

Seguindo uma linha de pesquisa semelhante, Roberto (2020) também almeja compreender este novo paradigma, porém sob a ótica da responsabilização civil nos casos de acidentes em carros autônomos regidos por sistemas de IA. Este será compreendido a partir da técnica “aprendizagem de máquina” e por isso, pode ser caracterizada por sua capacidade de auto aprendizagem e de tomar decisões autônomas. Este autor utiliza o enfoque “homem máquina” para caracterizar essas decisões automatizadas que, por serem consideradas independentes da vontade do fabricante quanto do usuário, com pouca ou nenhuma interferência humana ou produzidas muitas pessoas concomitantemente, encontra dificuldades em encontrar subsunção nas regras do Código Civil acerca da responsabilização subjetiva e objetiva. Ao tentar aplicar a ótica da responsabilidade subjetiva, este autor acredita que não cabe adentrar nas categorias de culpa por não ser possível identificar o sujeito de atuação para estabelecer uma relação causal entre suas ações e danos. Ademais, por essas decisões serem usualmente difusas e opacas quanto a sua operabilidade, a aplicação de responsabilidade objetiva se torna ainda mais inapropriado. Logo, faz uma analogia destas tomadas de decisões autônomas aos “bugs de software”, visto que ambos são até certo ponto inevitáveis e apresentam um risco inerente e que não pode ser completamente extinto. Verifica que, nos sistemas de IA, existe um risco de autonomia inerente que as leis atuais não abarcam e por isso, sugere uma discussão pela sociedade e autoridades reguladoras para definir em que medida o direito civil deve responder a este novo paradigma de responsabilização.

No âmbito externo existe um debate recente envolvendo esta temática. Em

27 de fevereiro de 2020, o Tribunal Administrativo da Corte Francesa realizou a primeira decisão acerca da aplicação do reconhecimento facial. Para compreender melhor o caso, em dezembro de 2018, duas escolas do ensino médio francesas, uma localizada em Marseille e outra localizada em Nice, decidiram utilizar câmeras nos portões da escolas para permitir a entrada de alunos para aumentar a segurança e dar maior fluidez ao tráfego, como forma de substituir os cartões de identificação. Esta medida foi contestada judicialmente, entretanto, na primeira instância foi decidido pela legalidade da aplicação do reconhecimento facial nas escolas. Em fevereiro de 2019, a associação "La Quadrature du Net", a Liga dos Direitos do Homem e a Federação dos Conselhos de pais de alunos das escolas públicas dos Alpes Marítimos contestaram a sentença. Foi alegado que a utilização deste tipo de biometria, traria grandes riscos à privacidade e liberdade políticas - especialmente por envolver menores de idade. Durante o julgamento, agora na segunda instância, a corte francesa aplicou a lei de proteção de dados no uso do reconhecimento facial. Ao final do julgamento, a corte superior reconheceu que esta deliberação não respeitou a privacidade dos alunos uma vez que os mesmos não consentiram de uma maneira clara e livre pela utilização destes dados. Sua decisão foi fundamentada nestes principais pressupostos: apesar de existir documentos que atestaram o consentimento, seja pelos próprios alunos ou no caso de menores, por seus representantes legais, a corte determinou que a mera assinatura num formulário não era suficiente para utilizar a tecnologia, e o fato dos alunos estarem sob a direção das escolas não oferece nenhum tipo de garantia de que o consentimento foi dado de forma livre e informada; e, em termos de proporcionalidade, a utilização desta tecnologia foi considerada desproporcional frente a outras alternativas e desrespeitando princípio da "minimization of data", que diz respeito a postura que o controlador do banco de dados deve ter para acessar somente dados pessoais estritamente necessários e relevantes para cumprir seus objetivos, e isso inclui o período de retenção de dados para este mesmo propósito. (CHRISTAKIS, 2020)

Dado este diagnóstico, em que ramos da ciência aparentemente diferentes compartilham o mesmo espaço científico e questionamentos sobre suas abordagens paradigmáticas, é fundamental delimitar este tema a partir da Lei Geral de Proteção de Dados (LGPD), conhecida como Lei nº 13.709/2018, pois, mesmo não tratando diretamente do sistema IA, sua regulação impacta diretamente no seu uso e desenvolvimento.

Se tratando desta ramo da pesquisa, o recorte do tema foi realizado tendo em vista a importância que a Lei Geral de Proteção de Dados vem adquirindo. Neste sentido, cabe dar atenção especial aos pressupostos e limites das teorias jurídicas atuais que possuem incipiente produção acadêmica neste tema. Logo, se trata de uma pesquisa contemporânea, sobretudo com o enfoque do consentimento.

Queiroz (2011) indica três exemplos de como transformar um tema em um problema de pesquisa. Este autor sugere que um n de pesquisa jurídica tem como objetivo: buscar uma resposta nova para uma pergunta antiga; buscar organizar ou sistematizar um tema recente ou determinar o significado jurídico de alguma inovação. Verifica-se que este trabalho tem como problema: a LGPD não estabelece o reconhecimento facial como um setor específico de uso da IA e que, por usar dados sensíveis, esta lacuna acarretará riscos à privacidade de dados dos cidadãos. Seguindo

a classificação de Queiroz (2011), este trabalho possui um problema propositivo, ou seja, um problema que visa ir além do diagnóstico descritivo, e por isso buscará sistematizar um tema recente. Por isso, esta pesquisa tem como pergunta: Como o uso do reconhecimento facial deve ser analisado diante da ausência normativa na LGPD? A hipótese deste trabalho é que possível analisar a experiência europeia no que tange a aplicação da Regulação Geral de Proteção de Dados da União Europeia (RGPD) e realizar breves apontamentos sobre as atuais teorias de responsabilidade civil. A partir desta abordagem metodológica, especialmente baseada em Queiroz (2011), estas informações serão transformadas e selecionadas a fim de se tornarem úteis, especialmente para aqueles que almejam trabalhar com este tema. De maneira sintética, e aplicando aos objetivos específicos deste trabalho, possível responder a seguinte pergunta: Como definir reconhecimento facial, uma vez que a LGDP, e de maneira que a segurança pública possa utilizar essa tecnologia sem afetar vida privada?

A metodologia utilizada será o método indutivo cujo objetivo é chegar a conclusões mais amplas do que o conteúdo estabelecido pelas premissas de base. O procedimento de pesquisa será do tipo pesquisa descritiva aplicando a técnica de coleta de dados chamada análise bibliográfica. E as conclusões não são buscadas de forma apriorística, logo, elas devem resultar da análise de fenômenos recorrentes. Por isso, tem como base uma generalização de propriedades semelhantes que podem ser observados em ocorrências de fatos similares.

Num primeiro momento, é possível prever que, devido ao perfil deste trabalho, haverá escassez de material científico nacional no que tange ao tema direito e inteligência artificial. Por isso, algumas das informações divulgadas pela administração pública europeia, dentre elas FORUM (2020); BOARD(2020), e nos veículos de comunicação nacionais, dentre eles Nakagawa (2020), Lemos (2020), Roberto e Lopes (2020), serão utilizados; Esta discussão, todavia será aproximada tanto dos livros acadêmicos quanto publicações em periódicos. A coleta de dados será realizada tendo em vista o encadeamento dos argumentos dos principais autores em questão, a partir de cada obra analisada, especialmente Almada e Dymitruk (2020), Almada (2020), Selinger, Evan and Hartzog (2020) e Roberto (2020). Essa forma de análise de resultados se dará com base na discussão que cada autor traz, extraindo as principais repercussões que seu diálogo gera com o objeto desta pesquisa.

1. MÉTODO DO DIREITO COMPARADO E INTELIGÊNCIA ARTIFICIAL

Dutra (2020) conclui em seu artigo que, a pluralidade que caracteriza o Direito Comparado faz parte essencial do processo de pesquisa em torno desta disciplina, podendo não só ser aplicada de maneira individual ou conjunta, mas de acordo com os interesses do objeto pesquisado. Assim, esta disciplina que possui um rol de métodos considerados não excludentes. Ao contrário –quando bem aplicados de forma conjunta, contribuem de maneira fundamental para sofisticar a pesquisa científica. Ao mesmo tempo, a escolha do método a ser utilizado não é impositiva, podendo variar de acordo com os interesses do pesquisador. Esses interesses, por sua vez, são resultado de fatores que são tanto internos quanto externos à pesquisa, e que veem na pluralidade dos métodos um importante aliado para a construção de uma produção acadêmica com resultados que são não só mais produtivos e confiáveis,

mas também mais eficazes em seu aproveitamento no campo da prática jurídica.

Por isso, novas perspectivas relacionada aos métodos do direito comparado são bem vistas pois contribuem para que essa disciplina continue a ser, cada dia mais, um significativo campo do direito num mundo cada vez mais internacionalizado. Logo, é interessante observar que é necessário obter uma análise de direito comparado sobre questões que envolvem inteligência artificial, especialmente acerca da Lei Geral de Proteção de Dados.

2. RECONHECIMENTO FACIAL: NOTAS INICIAIS SOBRE O OBJETO

2.1 RECONHECIMENTO FACIAL: ALGORITMOS E FUNCIONALIDADES

Algoritmos, como um aspecto fundamental de todos os sistemas de IA, fazem parte dos softwares, que coordenam uma série de programas que visam para realizar um cálculo ou resolver um problema. Software biométrico é um grupo de tecnologias que traz uma tecnologia exclusiva para cada indivíduo, e pode incluir impressões digitais, mãos, olhos, reconhecimento facial, voz, modos de caminhar, assinatura, e que também podem ser usados para autenticar o indivíduo. Os algoritmos mais amplamente utilizados para reconhecimento facial são o DeepFace, criado pelo Facebook em 2014, e o FaceNet, criado pelo Google em 2015. (WEF Framework, 2020). Agora, o reconhecimento facial é um software biométrico capaz de confirmar a identidade de uma pessoa usando uma análise de dados baseada em padrões dessa geometria facial, denominada regularmente modelos (Diretrizes da EDPB 3/2019).

O objeto reconhecimento facial precisa ser contextualizado em três processos principais. Por esse motivo, será agregado alguns conceitos essenciais para entender como um software biométrico funciona. Como a imagem captada é submetida a um sistema de reconhecimento facial para ser comparada a indivíduos inscritos, ela pode ser convertida em *templates*, que são recursos interpretados por uma máquina extraídos de uma ou mais imagens de um indivíduo para criar uma imagem completa do indivíduo. É possível dizer que o *template* é a identificação exclusiva dos indivíduos e a imagem captada é uma versão dessa identificação individual. A inscrição consiste em um sistema de verificação usado para autenticação. O *template* também pode estar associado a um identificador primário que será usado para determinar o modelo de análise. Durante o processo de funcionamento do software biométrico, pode ocorrer um falso negativo, que é um resultado de teste que diz incorretamente que o indivíduo nessa imagem capturada - aquela que é submetida ao teste - não está registrada ou não corresponde ao banco de dados de imagens. Outro fenômeno que pode acontecer é um falso positivo, que é quando o teste indica de maneira incorreta que o indivíduo na imagem da sonda é armazenado no sistema quando na verdade não é. Perceba que mesmo o falso negativo e o falso positivo têm consequências diferentes. Como o primeiro indicou incorretamente que a imagem capturada não está na base de dados, a segunda indica que a imagem capturada está no banco de dados, mas de maneira incorreta.

Esta passagem trabalhou em conceitos de algoritmos baseados em conceitos de imagem capturada, *template*, falso positivo e falso negativo e as suas funcionalidades visando preparar o leitor para o tópico sobre os modos de aplicação desta

2.2 RECONHECIMENTO FACIAL: MODOS DE APLICAÇÃO

Fundamentalmente, um processo chamado verificação de rosto é usado em cenários de segurança em que a verificação depende da existência de um identificador primário (como um ID de cliente) e o software biométrico é usado como um segundo fator para verificar a identidade da pessoa. O algoritmo faz uma verificação de correspondência denominada “um para um”: o modelo extraído naquele momento é comparado ao modelo armazenado para verificar a pessoa associada à identificação apresentada, a fim de responder à pergunta: “Essas duas imagens são a mesma pessoa?” .

Existe um processo semelhante, chamado identificação de face, ou seja, quando o software biométrico tenta corresponder um modelo de análise a todos os modelos de inscrição armazenados em um repositório, também chamado de correspondência "um para muitos". O algoritmo faz uma verificação de correspondência com base na precisão com que o modelo extraído naquele momento corresponde a cada um dos modelos registrados, para responder à pergunta: “Essa pessoa desconhecida pode corresponder a um modelo registrado?”.

Portanto, por mais simples que possa parecer, mesmo a detecção de um rosto, que visa responder a seguinte pergunta: “Há um ou mais rostos humanos nesta imagem?” possui diferentes formas de identificação. Logo, a regulamentação do uso de qualquer um desses processos de identificação, precisa levar em consideração estas peculiaridades. Portanto, é importante certificar que a precisão do reconhecimento facial se baseia em duas condições: (1) com que frequência o sistema identifica corretamente uma pessoa que está registrada no sistema; e (2) com que frequência o sistema não encontra correspondências corretamente para uma pessoa que não está registrada. (Estrutura WEF, 2020)

2.3 RECONHECIMENTO FACIAL: REFLEXÕES SOBRE PRIVACIDADE E A SUA REGULAÇÃO

Nem todo mundo se sente à vontade com a vigilância por vídeo. Mas a realidade mostra que cada vez mais estão sendo implementadas ferramentas que conseguem explorar imagens capturadas em fotografias tradicionais, como em um baile de formatura, ou em câmeras inteligentes, como as próximas à campainha das residências. É por isso que a questão da vigilância por vídeo é delicada. Essas técnicas, que podem ser mais invasivas (por exemplo, usando tecnologias biométricas complexas) ou menos invasivas (por exemplo, algoritmos simples de contagem de fotos), permanecem desconhecidas para a maioria dos usuários. A quantidade de dados gerados pelo vídeo, combinada com essas técnicas biométricas, aumenta os riscos de uso secundário por agentes de má fé. E mesmo os princípios gerais descritos no artigo 5º do RGPD, podem não ser suficientes para lidar com os riscos de uso indevido, relacionados ou não ao objetivo originalmente atribuído ao sistema (Diretrizes EDPB 3/2019). Atenção ao fato de o GDPR não ser o único regulamento europeu sobre o processamento de dados pessoais por meio de dispositivos de vídeo. Existe

uma Diretiva de Aplicação da Lei, LED (EU2016/680), que autoriza o processamento de dados pessoais pelas autoridades competentes para fins de impedir, investigar, detectar ou processar ofensas criminais ou aplicar sanções penais. Essa regulamentação subsidiária não ofende a RGPD, porque esta legislação também permite esse uso sob requisitos específicos desta legislação europeia. (Diretrizes EDPB 3/2019).

Observe que se um indivíduo não puder ser identificado, direta ou indiretamente, esses dados não se enquadram em nenhum dos regulamentos europeus. Em geral, ele não cobre "câmeras falsas", que correspondem a qualquer câmera que não esteja funcionando como uma câmera e, portanto, não está processando dados pessoais; um exemplo que pode ser citado e a câmera de vídeo é integrada ao carro para fornecer assistência ao estacionamento. Além disso, existe a "exceção de *household*", que diz respeito às gravações que são feita por indivíduos durante a sua vida privada e que claramente não foram produzidas para serem divulgadas pela *internet* e estarem acessíveis a um grande número de pessoas. Não menos importante, o armazenamento de dados destas tecnologias pode ser feito através de soluções de caixa preta, nas quais as imagens são excluídas automaticamente após um determinado período de armazenamento e acessadas apenas em casos extremos; ou simples monitoramento em tempo real sem armazenamento. Logo, depreende-se que se a câmera for construída ou ajustada de forma que não tenha como objetivo principal coletar informações relacionadas ao indivíduo, o GDPR não será aplicado. (BOARD, 2020)

Por esses motivos, para fornecer uma estrutura adequada aos métodos e conceitos digitais existentes, este tópico apresenta alguns elementos da ciência da computação para preparar os profissionais do direito a compreender essa temática. Para este projeto, é necessário introduzir esses conceitos em total compreensão antes de tentar aplicar questões legais, especialmente no que tange a ideia de responsabilidade, conforme será demostrado nos tópicos a seguir.

3. REGULAMENTAÇÃO SOBRE RECONHECIMENTO FACIAL NO BRASIL: INICIATIVAS BRASILEIRAS E NOVOS PARADIGMAS

O termo reconhecimento facial, possuidor de peculiaridades por utilizar dados pessoais sensíveis e sistemas de IA, não possui regulamentação específica dentro da LGDP. E, este tipo de lacuna legislativa merece ser analisado a partir de um enfoque ético do consentimento pois pode gerar impactos não abarcados pelas teorias jurídicas atuais. Por isso, esse vácuo legislativo proporciona um espaço para analisar como o direito civil, e especialmente a responsabilidade civil, pode responder o uso reconhecimento facial sem consentimento.

Esforços devem ser concentrados sobre a Lei nº 13.709/2018 por ser a lei mais vocacionada a estabelecer uma espécie de regulação do ecossistema de algoritmos. Dela, vamos extrair o conceito de dados pessoais sensíveis que corresponde, conforme artigo inciso II do artigo 5º da referida lei, a 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.

Ao abordar a definição de dados pessoais sensíveis, alguns aspectos devem ser esclarecidos: esta categoria é visada a receber proibição absoluta ou limitação de coleta e uso de dados neste ecossistema de algoritmos. Sua proteção, para situações que não estão previstas na LGPD, pode ocorrer através de "zonas não conectadas" em ambientes críticos, como menores em ambiente escolar ou de indivíduos exercendo sua intimidade privada. Ainda, deve ser levado em conta que nem todo dado pessoal se refere a um dado exclusivo da vida da pessoa, ou seja, nem sempre a utilização de um banco de dados pessoais estará invadindo a privacidade de uma pessoa. Porém, isso não quer dizer que a proteção de dados está subjugada na categoria processamento de dados. Eventualmente, este debate pode se tornar acirrado especialmente quando o processamento de dados que utiliza dados pessoais e feito em operações realizadas por autoridades da segurança pública (ALMADA; DYMITRUK 2020).

Note que esta definição legal contempla dados biométricos. Considerando que a LGPD se espelha na regulamentação europeia vale ressaltar que a RGPD agrega a definição de dados biométricos uma espécie de junção de medições que, de acordo com o artigo 4.14: "é resultado de um processamento técnico específico relacionado às características físicas, fisiológicas ou comportamentais" (tradução livre). Ou seja, as imagens de vídeo de um indivíduo não podem ser consideradas dados biométricos, elas precisam ser tecnicamente processadas para identificação de um indivíduo. Assim, a RGPD considera basicamente três critérios: a natureza dos dados - características físicas, fisiológicas ou comportamentais; meios e forma de processamento e o objetivo único de identificar uma pessoa física. (BOARD, 2020).

Observe que esta definição não qualifica como dados pessoais sensíveis e, no que tange o artigo 9 da RGPD, se não tiverem sido especificamente tratados para identificar um indivíduo, esses dados não podem ser considerados dados biométricos. Portanto, para iluminar esta complexidade, três fases de processamento devem ser considerados: natureza dos dados (dados relativos às características físicas, fisiológicas ou comportamentais de uma pessoa natural); meios e forma de processamento (dados "resultantes de um processamento técnico específico) e finalidade do processamento (os dados devem ser utilizados com a finalidade de identificar exclusivamente uma pessoa singular). Nesta visão, não podemos esperar que o vídeo privado caseiro possa ser fonte de dados biométricos porque não são processados nos critérios. Portanto, além da necessidade dessas três características, esses elementos precisam passar por essas três fases para identificar de maneira única a pessoa.

Depois, após discriminar esses elementos e a fim de compreender uma definição de dados biométricos, será conjugado os principais elementos dessas duas leis, respeitando cada peculiaridade das diferentes descrições apresentadas. Para apresentar um resultado analítico, este artigo consagra a seguinte definição de reconhecimento facial:

Definição 1. Reconhecimento Facial são dados pessoais sensíveis, com processamento técnico específico relacionado às características físicas, fisiológicas ou comportamentais.

Após apresentar este resultado analítico aproximado do RGPD e sua lei similar no Brasil, denominada LGPD, este artigo trará algumas considerações e os desafios que a falta de regulamentação sobre este tipo de tecnologia pode enfrentar.

4. DESAFIOS REFERENTES A RESPONSABILIZAÇÃO PELO USO DE RECONHECIMENTO FACIAL

Considerando que os dados biométricos são dados pessoais sensíveis, é interessante verificar as principais notas sobre o tratamento desses dados. Tepedino et Frazao (2019) organizou artigos interessantes sobre LGPD. Ao abordar a modalidade de processamento de dados, que não deve ser confundida com o "direito a ser esquecido", verificou-se que a responsabilidade civil pelas operações de exclusão de dados, quando ocorre após o término do processamento pode ser, mesmo que a LGPD opte para um regime de natureza subjetiva, a cláusula geral de responsabilidade pelo risco contida no único parágrafo do art. 927 do Código Civil. Especialmente no que tange ao direito de ser esquecido, trata-se do direito do indivíduo de se opor à lembrança pública e opressiva de fatos que não refletem mais sua identidade pessoal, mas que não está presente na LGPD. Essa legislação brasileira, por sua vez, tem, como a RGPD, o direito de excluir dados, uma prerrogativa inspirada na dignidade da pessoa humana. Ao tratar de segurança e confidencialidade dos dados pessoais no LGPD, uma vez que não foram tratados pelo Código de Proteção ao Consumidor, é necessário que a implementação de padrões de segurança seja realizada não apenas pelos controladores destes dados, mas também por qualquer pessoa que execute o processamento de dados, seja em qualquer uma de suas fases. Nesse sentido, cabe o conceito de privacidade por design, contemplado no diploma, garantindo que a segurança e a confidencialidade dos dados sejam elementos centrais no design, desenvolvimento, aplicação e avaliação de produtos e serviços.

Pedro, Selle e Vieira (2020) possuem como objeto o uso “inteligência artificial visual”, um sistema desenvolvido por pesquisadores que capaz de reconhecer padrões visuais, com foco em padrões faciais para sistemas de segurança e navegação de vídeo. Sua aplicação serve tanto para objetos parcialmente cobertos como reconhecimento automático de objetos em supermercados utilizando dados biométricos. Assim, ao tratar de aplicação da inteligência artificial na indústria da moda, especialmente quando utilizado por fabricantes de produtos têxteis, e necessário conjugam diversas de legislações, entre elas a Constituição da República Federativa Brasileira, o Código Civil, o Código de Defesa do Consumidor, o Marco Civil da *Internet* e a Lei Geral de Proteção de Dados para responsabilizar aquele que viola essa garantia quando da utilização dos dados coletados por meio de IA. Além disso, ao identificar os dispositivos legais e a jurisprudência aplicável para a proteção de dados, estes autores demonstram a falta de abordagem específica para este tema. Estes autores também explicitaram a atuação dos tribunais superiores neste âmbito. A ministra do Nancy Andrighi, do Superior Tribunal de Justiça (STJ) no Recurso Especial 1.694.405/RJ, utiliza o artigo 19 da da Lei 12.965/2014, ao interpretar que assim que houve a notificação judicial que ordena a retirada de determinado conteúdo da *internet* começa a ensejar a possibilidade de ressarcimento do ato lesivo de publicação de conteúdo indevido. Neste mesmo sentido, o entendimento do ministro Luis Felipe Salomão, ministro do STJ, no Recurso Especial 1.512.647/MG, considera que apenas quando o provedor de *internet* permanecer inerte, após notificado, ensejará responsabilizado

pelos danos concretizados. No caso de se tratar de circunstância lesiva ao direito autoral, a ordem que determina a retirada do conteúdo da *internet*, além de ser proveniente do Poder Judiciário, deve ser identificada claramente e especificamente no seu conteúdo, através do seu endereço URL, sob pena de nulidade, para obter o requisito de validade. Logo, denota-se que o posicionamento jurisprudencial brasileiro possui passagens sobre a aplicação de responsabilização civil que circundam a temática proteção de dados, especialmente no que tange às sociedades empresárias provedoras de dados pessoais.

As pesquisas mais recentes sobre este assunto, já questionam busca do governo para regular questões de consentimento acerca do uso deste tipo de tecnologia para vigilância. Selinger e Hartzog (2020) acreditam que solicitar o consentimento individual visando proteger rostos de serem rastreados e etiquetados muito provavelmente não serão cumpridas. Este tipo de tecnologia possui um problema de consentimento intrínseco devido a sua própria estrutura de captação de dado biométrico. Logo, esta captação transcende o consentimento individual válido. E mesmo se possível, existem interesses públicos e "interesses obscuros" que podem dificultar esta intermediação. Por isso, estes autores acreditam que o consentimento dificilmente pode anteceder o uso de tecnologias de reconhecimento facial, seja apenas caracterização, verificação e identificação. Lemos (2020) caracteriza melhor ao abordar esta questão do (não) consentimento, ao estabelecer que não estamos tratando de mero cadastro de imagens ou fatos, e sim de um dado biométrico de identificação, pois a geometria facial e utilizada como se fosse uma identidade, única para cada indivíduo. Este tipo de tecnologia, a partir de uma imagem individualizada da pessoa, gera uma categorização de indivíduos. Porém, apesar de ser uma autenticação bastante segura, sua coleta e demasiadamente acessível e, muitas vezes prescinde do consentimento do indivíduo.

Para entender a possibilidade de aplicar uma teoria da responsabilidade civil no que diz respeito ao uso de dados e que envolvem algoritmos, é possível abordar os paradigmas que envolvem a responsabilidade civil pelo uso de sistemas de inteligência artificial. Roberto (2020), ao abordar a responsabilidade por decisões autônomas independentes, traz uma análise interessante sobre um projeto de pesquisa em uma universidade sueca realizado em 2002. O projeto do robô Gaak é caracterizado por possuir vários animais robóticos que foram treinados para atuar como "presa" e "caçadores". A partir desses testes, a ideia era analisar a hipótese evolutiva de sobrevivência do mais apto e liberar os robôs para desenvolver estratégias de sobrevivência por si mesmos. O desempenho desses animais-robôs foi caracterizado basicamente pela presa procurando pontos de luz que foram interpretados como "comida" e pelos caçadores tentando capturar a presa. No entanto, um dos prisioneiros, por razões desconhecidas, começou a circundar a grade do espaço de testes, encontrou uma brecha, escapou, atravessou uma estrada próxima e foi quase atropelado por um motorista que estava dirigindo para lá. Este exemplo de decisão autônoma pode ocorrer, tanto em animais robóticos quanto em animais reais. Uma sugestão que Roberto (2020) administra é que essa nova categoria de risco social, de acordo com a literatura pesquisada por ele, significa que seria necessário um novo tipo de responsabilidade objetiva, baseada principalmente na noção de "criar um perigo" ou " implementação de um robô ". É muito semelhante à responsabilidade civil pelo

comportamento dos animais, à responsabilidade dos responsáveis pelos atos dos agentes e até, em referência à lei romana antiga, à responsabilidade pelos atos dos escravos. No entanto, após breve verificação em vários trabalhos, ele observa que a exploração completa dessas propostas e seus possíveis resultados exigiria uma tese em si e, possivelmente, a criação de um novo tipo de capacidade ou personalidade jurídica para os próprios sistemas de inteligência artificial. Nesse sentido, fica claro que existe um vazio legislativo na regulamentação desta hipótese de responsabilidade civil nos casos que envolvem o uso da tecnologia.

5. CONCLUSÃO

A partir destes tópicos, é possível concluir que, para que o reconhecimento facial seja utilizada no Brasil, seria necessário, além de suprir este vácuo legislativo sobre a definição deste objeto, uma hipótese em que caso seja utilizada pelo setor público sem consentimento, haja a devida responsabilização do agente. Assim, podemos observar que o cenário brasileiro, está focado em regular políticas públicas para sua maior adoção e estímulo ao investimento do que na regulação de suas práticas, especialmente no que tange a utilização por autoridades policiais. Em contrapartida, no âmbito externo, especificamente na Europa, a tecnologia reconhecimento facial, além de ser utilizada, possui legislação própria, estudos para sua aplicação e jurisprudência. É possível observar que, questões de consentimento estão gerando repercussões tanto nos projetos de lei nacionais quando na aplicação de leis no ambiente externo. Por isso, mesmo que a LGDP possibilite a regulação posteriormente normas sobre alguns aspectos mais polêmicos, a falta de uma regra exclusiva acerca da responsabilização do uso do reconhecimento facial, especialmente no que tange ao certo grau de autonomia destes sistemas, pode ser se tornar um problema num futuro não muito distante. Por isso, enquanto não se desenvolve um novo paradigma para este tipo de responsabilização de IA, especificamente no que tange ao reconhecimento facial, este artigo buscou definir, a partir da aplicação do método de direito comparado sobre a regulamentação europeia, alguns parâmetros para suprir o vácuo legislativo acerca da definição reconhecimento facial.

Uma vez que a LGPD não estabelece o reconhecimento facial e como um setor específico de uso da IA existe o risco de que a mesma venha a ser utilizada por setores da sociedade e sem consentimento. Além disso, este uso pode ser considerado de alta gravidade pois a partir de decisões automatizadas que o reconhecimento facial se utiliza, é possível obter *templates* faciais errados e ocasionar acidentes, especialmente se for feita sem uma base de dados robusta. Assim, este artigo sugere que caso o setor público tenha uma base de dados que contemple a região dos olhos, seria possível que se utilizasse da tecnologia reconhecimento facial, mesmo que sem consentimento.

O uso dessas tecnologias deve respeitar os princípios da legalidade, necessidade, proporcionalidade e minimização de dados. E mesmo sendo considerado eficaz, os controladores que manipulam estes dados devem avaliar o impacto sobre os direito e liberdades que terão sobre o processamento destes dados pois, para se qualificar como dados biométricos, é necessário que essa coleta de dados brutos, que levam em conta as características físicas, fisiológicas e comportamentais da pessoa física, implicam na medição destas características.

O estudo do reconhecimento facial, sob a perspectiva da proteção de dados, precisa levar em conta um enfoque ético do (não) consentimento pois, considerando que os reconhecimento facial, que utiliza dados biométricos classificados como dados pessoais sensíveis, o uso dessa tecnologia devem ser exclusivo para garantir a segurança do titular ou questões de interesse público.

Finalmente, este trabalho teve como produto, além dos apontamentos acima levantados, a definição sobre o reconhecimento facial como dados pessoais sensíveis e dotados de processamento técnico específico relacionado às características físicas, fisiológicas ou comportamentais pode servir de parâmetro para os futuros projetos de lei que envolvam a temática direito e inteligência artificial

REFERÊNCIAS BIBLIOGRÁFICAS

ALMADA, Marco. Artificial Intelligence: Perspectives from Legal Philosophy. Disponível em: https://www.researchgate.net/publication/328393397_Inteligencia_Artificial_Perspectivas_a_partir_da_Filosofia_do_Direito/link/5c884f29299bf14e7e78292a/download. Acesso em: 18 maio 2020.

ALMADA, Marco; DYMITRUK, Maria. Privacy and Data Protection Constraints to Automated Decision-Making in the Judiciary. Disponível em: https://www.researchgate.net/publication/340594815_Privacy_and_Data_Protection_Constraints_to_Automated_Decision-Making_in_the_Judiciary#pf2. Acesso em: 21 maio 2020.

BOARD, Europa Data Protetion (org.). Guidelines3/2019 on processing of personal data through video devices. Disponível em: Guidelines 3/2019 on processing of personal data through video devices https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_201903_videosurveillance.pdf. Acesso em: 21 maio 2020.

BRASIL. Lei Geral de Proteção de Dados Pessoais (LGPD). . Brasília, Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 15 maio 2020.

CHRISTAKIS, Theodore. First Ever Decision of a French Court Applying GDPR to Facial Recognition. Disponível em: https://ai-regulation.com/first-decision-ever-of-a-french-court-applying-gdpr-to-facial-recognition/. Acesso em: 19 maio 2020.

DUTRA, Deo Campos. MÉTODO(S) EM DIREITO COMPARADO. Disponível em: https://revistas.ufpr.br/direito/article/view/46620/29831. Acesso em: 06 out. 2020.

FORUM, World Economic (org.). A Framework for Responsible Limits on Facial RecognitionUse Case: Flow Management. Disponível em: http://www3.weforum.org/docs/WEF_Framework_for_action_Facial_recognition_2020.pdf. Acesso em: 20 maio 2020.

VARGAS, Fundação Getúlio Vargas (org.). Sumário Executivo da Pesquisa Quantitativa "TECNOLOGIA, PROFISSÕES E ENSINO JURÍDICO". São Paulo: Fundação Getúlio Vargas, 2018. Disponível em: https://www.academia.edu/39575635/Sum%C3%A1rio_Executivo_da_Pesquisa_Qualitativa_TECNOLOGIA_PROFISS%C3%95ES_E_EN-

SINO_JUR%C3%8DDICO_. Acesso 7 jun de 2020.

NAKAGAWA, Liliane. Reconhecimento facial deverá ser informado ao consumidor. Disponível em: https://olhardigital.com.br/noticia/reconhecimento-facial-devera-ser-informado-ao-consumidor/89491. Acesso em: 17 maio 2020.

PEDRO AF, SELLE YP, Vieira PRS. A Responsabilidade Civil Pelo Uso de Dados na Indústria da Moda. Rev Prop. Intelec. Online. 2019/2020 set./fev.; 2(2):111-116

LEMOS, Simone. RECONHECIMENTO facial: novo sistema biométrico de identificação. Disponível em: https://jornal.usp.br/atualidades/reconhecimento-facial-novo-sistema-biometrico-de-identificacao/. Acesso em: 10 maio 2020.

ROBERTO, Enrico. Responsabilidade civil pelo uso de sistemas de inteligência artificial: em busca de um novo paradigma. Disponível em: https://revista.*internet*lab.org.br/responsabilidade-civil-pelo-uso-de-sistemas-de-inteligencia-artificial-em-busca-de-um-novo-paradigma-2/. Acesso em: 21 maio 2020.

ROBERTO, Enrico; LOPES, Marcelo Frullani. Quando um carro autônomo atropela alguém, quem responde? Disponível em: https://brasil.elpais. com/brasil/2018/04/16/tecnologia/1523911354_957278.html. Acesso em: 21 maio 2020.

SELINGER, Evan and HARTZOG, Woodrow, The Inconsentability of Facial Surveillance Disponível em: https://ssrn.com/abstract=3557508 . Acesso em: 17 maio 2020.

QUEIROZ, Rafael Mafei Rabelo. (2011). Artigo Científico: Concepção, Temas, Métodos e Técnicas. BePressSelected Works. Disponível em: http:// works.bepress.com/rafaelmafei.